

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ

Руководитель направления

проф., д.т.н., доц.

(должность, уч. степень, звание)

С.В. Беззатеев

(инициалы, фамилия)



(подпись)

«26» мая 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы теории сложности»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Безопасность компьютерных систем
Форма обучения	очная

Санкт-Петербург– 2022

Аннотация

Дисциплина «Основы теории сложности» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-1 «Способен определять состав программно-аппаратных средств защиты информации в операционных системах»

ПК-2 «Способен определять состав программно-аппаратных средств защиты информации в компьютерных сетях»

ПК-3 «Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований»

Содержание дисциплины охватывает круг вопросов, связанных с вопросами теории сложности вычислений, определения и свойства математических объектов, используемых в этой области, формулировки утверждений, методы их доказательства, возможные сферы их приложений.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью преподавания данной дисциплины является ознакомление с теорией сложности вычислений, определения и свойства математических объектов, используемых в этой области, формулировки утверждений, методы их доказательства, возможные сферы их приложений.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-1 Способен определять состав программно-аппаратных средств защиты информации в операционных системах	ПК-1.3.1 знает принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы
Профессиональные компетенции	ПК-2 Способен определять состав программно-аппаратных средств защиты информации в компьютерных сетях	ПК-2.У.1 умеет оценивать угрозы безопасности информации в компьютерных сетях
Профессиональные компетенции	ПК-3 Способен применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств защиты информации, способен к использованию и внедрению результатов исследований	ПК-3.В.2 владеет навыками анализа научных данных, результатов экспериментов и наблюдений

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Базовые алгоритмы обработки информации,
- Алгоритмы и структуры данных.

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

- Теория автоматов и компиляторов.

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№4
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	17	17
Аудиторные занятия, всего час.	51	51
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)	17	17
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	36	36
Самостоятельная работа, всего (час)	21	21
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: ** кандидатский экзамен

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции и (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Раздел 1. Вычислительные модели и алгоритмы	6	3			5
Раздел 2. Np-полные задачи	8	4			5
Раздел 3. Результаты об Np-полноте	8	4			5
Раздел 4. Np-трудные задачи и подходы к решению Np-полных задач.	6	3			5
Раздел 5. За пределом класса Np-полных задач	6	3			6
Итого в семестре:	34	17			21
Итого	34	17	0	0	21

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Тема 1. Вычислительные модели и алгоритмы Определение машины Тьюринга. Функции вычислимые на машинах Тьюринга.. Определение недетерминированных машин Тьюринга. Функции вычислимые на недетерминированных машинах Тьюринга. Примеры функций вычислимых на машинах Тьюринга и недетерминированных машинах Тьюринга. Задачи распознавания языка и кодирование.
2	Тема 2. Np-полные задачи Полиномиальные алгоритмы: определение и примеры. Труднорешаемые задачи. Полиномиальная сводимость и эквивалентность. Примеры задач полиномиально сводящихся и полиномиально эквивалентных. Классы P и Np: определения и основные свойства. Соотношения между классами P и NP. Np-полные задачи. Теорема Кука.
3	Тема 3. Результаты об Np-полноте Основные Np-полные задачи: 3-выполнимость, трехмерное сочетание, вершинное покрытие, клика, гамильтонов цикл, разбиение. Методы доказательства Np-полноты: сужение задачи, локальная замена, построение компонент. Анализ подзадач. Задачи с числовыми параметрами и сильная Np-полнота. Примеры новых Np-полных задач.
4	Тема 4. Np-трудные задачи и подходы к решению Np-полных задач Оракульные вычисления и сводимость по Тьюрингу. Определение Np-трудных задач и их основные свойства. Приближенные алгоритмы: определения, примеры и основные свойства. Оценки погрешности приближенных алгоритмов. Применение теории Np-полноты к отысканию приближенных решений. Примеры приближенных алгоритмов для решения "трудных" задач.
5	Тема 5. За пределом класса Np-полных задач Структура класса Np. Полиномиальная Иерархия, проблема о невырожденности полиномиальной иерархии. Алгоритмическая сложность задач перечисления. Полнота с полиномиально ограниченной памятью. Логарифмическая память. Примеры задач разрешимых с полиномиально ограниченной памятью, разрешимых с логарифмически ограниченной памятью.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 4					

1	Функции вычислимые на недетерминированных машинах Тьюринга.	Решение задач	3	3	1
2	Нр-полные задачи.	Решение задач	4	4	2
3	Оценки погрешности приближенных алгоритмов	Решение задач	4	4	3
4	Применение теории Нр-полноты к отысканию приближенных решений	Решение задач	3	3	4
5	Примеры задач разрешимых с полиномиально ограниченной памятью, разрешимых с логарифмически ограниченной памятью	Решение задач	3	3	5
Всего			17	17	

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено				
Всего				

4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 4, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	11	11
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Подготовка к промежуточной аттестации (ПА)	5	5
Всего:	21	21

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий
Перечень печатных и электронных учебных изданий приведен в таблице 8.
Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 М 87	Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие / Н. Н. Мошак, Т. М. Татарникова; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 121 с.	40
51(075) Б 93	Математическая логика [Текст]: учебное пособие / Д. В. Бутенина, В. М. Лагодинский; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2011. - 52 с.	55
519.6/.8 Л 17	Математические основы криптологии. Тесты простоты и факторизация [Текст]: учебное пособие / С. В. Лазарева, А. А. Овчинников; С.-Петербург. гос. акад. аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2006. - 64 с.	79
519.7 Е 78	Элементы дискретной математики: учебное пособие/И. Л. Ерош, В. В. Михайлов; С.-Петербург. гос. ун-т аэрокосм. приборостроения. - СПб: ГОУ ВПО "СПбГУАП", 2008.	164
519.6/.8 К53	Д. Кнут. Искусство программирования для ЭВМ. Т.2: Получисленные алгоритмы. М., Вильямс, 2005	22
004 К84	Крук Е.А., Линский Е.М. Криптография с открытым ключом. Кодовые системы. ГУАП, 2004.	20

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»
Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.
Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
	Не предусмотрено

8. Перечень информационных технологий
8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться

100- балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	<ul style="list-style-type: none"> – обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	<ul style="list-style-type: none"> – обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> – обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> – обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	Определение машины Тьюринга. Функции вычислимые на машинах Тьюринга..	ПК-1.3.1 ПК-2.У.1 ПК-3.В.2
2	Определение недетерминированных машин Тьюринга. Функции вычислимые на недетерминированных машинах Тьюринга	
3	Примеры функций вычислимых на машинах Тьюринга и недетерминированных машинах Тьюринга. Задачи распознавания языки и кодирование.	
4	Полиномиальные алгоритмы: определение и примеры. Труднорешаемые задачи.	
5	Полиномиальная сводимость и эквивалентность. Примеры задач полиномиально сводящихся и полиномиально эквивалентных.	
6	Классы P и Np: определения и основные свойства. Соотношения	

	между классами P и NP. Np-полные задачи. Теорема Кука.
7	Основные Np-полные задачи: 3-выполнимость, трехмерное сочетание, вершинное покрытие, клика, гамильтонов цикл, разбиение.
8	Методы доказательства Np-полноты: сужение задачи, локальная замена, построение компонент. Анализ подзадач.
9	Задачи с числовыми параметрами и сильная Np-полнота. Примеры новых Np-полных задач.
10	Оракульные вычисления и сводимость по Тьюрингу.
11	Определение Np-трудных задач и их основные свойства. Приближенные алгоритмы: определения, примеры и основные свойства.
12	Оценки погрешности приближенных алгоритмов. Применение теории Np-полноты к отысканию приближенных решений.
13	Примеры приближенных алгоритмов для решения "трудных" задач.
14	Структура класса Np. Полиномиальная Иерархия, проблема о невырожденности полиномиальной иерархии.
15	Алгоритмическая сложность задач перечисления. Полнота с полиномиально ограниченной памятью.
16	Логарифмическая память.
17	Примеры задач разрешимых с полиномиально ограниченной памятью, разрешимых с логарифмически ограниченной памятью.

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Не предусмотрено	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру

проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Вычислительные модели и алгоритмы

Раздел 2. Np-полные задачи

Раздел 3. Результаты об Np-полноте

Раздел 4. Np-трудные задачи и подходы к решению Np-полных задач.

Раздел 5. За пределом класса Np-полных задач

11.2. Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимися практических занятий:

- закрепление, углубление, расширение и детализация знаний при решении конкретных задач;
- развитие познавательных способностей, самостоятельности мышления, творческой активности;
- овладение новыми методами и методиками изучения конкретной учебной дисциплины;
- выработка способности логического осмысления полученных знаний для выполнения заданий;

– обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Требования к проведению практических занятий

В рамках практических занятий разбираются задачи, для решения которых требуется применение алгоритмов, разбираемых на лекциях.

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются: учебно-методический материал по дисциплине.

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины. Форма проведения текущего контроля – защита отчетов по лабораторным работам. Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя: экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой