Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 23.10.2023 17:10:49
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Декан факультета информационных технологий
/Д. Г. Демидов/
«30» августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Математическая логика и теория алгоритмов в программировании»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Направленность подготовки
«**Безопасность открытых информационных систем**»

Квалификация (степень) выпускника
Специалист по защите информации

Форма обучения
Очная

Год приема 2021

Москва 2021 г.

1. Цели освоения дисциплины

К **основным целям** освоения дисциплины **«Математическая логика и теория алгоритмов в программировании»** следует отнести:

- развитие у студентов навыков логического и математического мышления, способностей к самостоятельной творческой работе;
- формирование у студентов знаний, умений и навыков владения аппаратом математической логики и теории алгоритмов для решения задач;
- привитие навыков работы со сложными логическими конструкциями и использования методов теории алгоритмов для оценки эффективности применяемых в практической деятельности алгоритмов.

К **основным задачам** освоения дисциплины **«Математическая логика и теория алгоритмов в программировании»** следует отнести:

- подготовку обучающихся к осуществлению деятельности по администрированию процесса контроля производительности автоматизированных систем (АС) и программного обеспечения (ПО);
- администрированию процесса управления безопасностью АС и ПО;

2. Место дисциплины в структуре ООП специалитета

Дисциплина **«Математическая логика и теория алгоритмов в программировании»** относится к числу профессиональных учебных дисциплин базовой части Б.1.3 блока Б.1 основной образовательной программы специалитета.

Дисциплина «**Математическая логика и теория алгоритмов в программировании**»» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Основы информационной безопасности», «Математический анализ».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	**знать:** - основные понятия и методы математической логики; - элементы математической лингвистики и теории формальных языков; - основные понятия и методы элементов и теории алгоритмов; - основные понятия и термины систем счисления; - основные понятия языка логики; **уметь:** - применять математические методы при решении профессиональных задач повышенной сложности; - применять на практике методы математической логики; - уметь строить логические выражения в языке логики высказываний и изоморфные им графовые модели (в частности, используя дизъюнктивный и конъюнктивный базисы Буля); - применять на практике методы теории алгоритмов; - решать задачи алгебры логики;

		владеть: - навыками алгебры логики (пропозициональной и кванторной); - решения научных и практических задач математическими методами при решении профессиональных задач; - навыками решения задач алгебры логики.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **4** зачетных единицы, т.е. **144** академических часа (из них лекции - 36 часов, практических занятий - 36 часа, самостоятельная работа - 72 часа). Форма контроля – экзамен в 1 семестре.

Структура и содержание дисциплины «Математическая логика и теория алгоритмов в программировании» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Введение. Роль математической логики и теории алгоритмов в прикладных науках.

Историческая справка. Предмет, цель и содержание курса «Математическая логика и теория алгоритмов в программировании». Основные понятия и определения алгебры логики и теории алгоритмов. Концептуальный базис математической логики. Построение математической логики. Содержательно и формально построенные логики. Языки логики как реляционные системы.

Тема 1. Системы счисления. Формальные системы.

Понятие системы счисления. Позиционные системы счисления. Нетрадиционная фибоначчиева система счисления. Примеры перевода чисел из одной системы счисления в другую. Алфавит как множество дескриптивных, логических и вспомогательных символов. Синтаксис языковых выражений. Аксиоматика (система аксиом, система схем аксиом) как подсистема правильно построенных языковых выражений и правила вывода. Исчисления. Примеры исчисления высказываний и исчисления предикатов.

Тема 2. Логика высказываний.

Логика и исчисление высказываний. Классическое определение исчисления высказываний. Конструктивное определение исчисления высказываний. Другие аксиоматизации исчисления высказываний. Язык логики высказываний. Алфавит логики высказываний. Пропозициональные термы, логические связки и вспомогательные символы. Формулы логики высказываний как формализованный язык. Кванторная алгебра логики. Субъектно-предикатная структура простых высказываний. Предикаты. Кванторы и квантификация предикаторных формул. Представление кванторов логическими связками на конечном универсуме рассмотрения. Свойства кванторов. Правила эквивалентных преобразований формул кванторной логики. Предваренные и префексные формы.

Тема 3. Исчисление предикатов.

Язык логики предикатов. Синтаксис языка логики предикатов. Языковые выражения – термы и формулы. Семантики языка логики предикатов. Модель интерпретации. Логика и исчисление предикатов. Исчисление предикатов как формальная система. Задачи исчисления предикатов. Отношения логического следования и логической эквивалентности. Примеры аксиоматик и правил

вывода классической логики предикатов. Правила вывода в логике предикатов первого порядка. Методы вывода в классическом исчислении предикатов.

Тема 4. Модальная логика.

Основные понятия модальной логики. Синтаксис и семантика модальной логики. Схемы модальных формул. Бинарные отношения. Обзор других формально-логических моделей.

Тема 5. Немонотонные рассуждения и методы поиска.

Модифицируемые рассуждения и свойства немонотонных логик. Зацикливание немонотонных рассуждений и его преодоление. Стратегии немонотонного вывода в глубину и ширину.

Тема 6. Алгебра логики.

Булева алгебра логики. Язык алгебры логики. Задача Венна. Логические (булевы) функции как *n*-арные операции. Способы задания логических функций. Табличные задания булевых функций. Существенные и несущественные переменные. Равенство булевых функций. Эквивалентность. Разложение булевых функций по переменным. Классическое представление логических функций: ДНФ, КНФ. Каноническое представление логических функций: совершенная дизъюнктивная нормальная форма (СДНФ), совершенная конъюктивная нормальная форма (СКНФ). Эквивалентные преобразования логических функций.

Тема 7. Элементы нечёткой логики.

Алгебры и модели (реляционные системы). Алгебра множеств (алгебра Кантора). Упорядоченные, частично упорядоченные множества. Алгебра нечетких множеств. Основные понятия и определения. Нечёткие логические формулы. Основные операции над нечёткими множествами и их свойства.

Тема 8. Введение в теорию алгоритмов.

Исторический обзор. Цели и задачи теории алгоритмов. Практическое применение результатов теории алгоритмов. Формализация понятия алгоритма. Формальные модели, уточняющие понятие алгоритм. Блок-схемы алгоритмов.

Тема 9. Алгоритмические системы Тьюринга, Черча и Маркова. Алгоритмически неразрешимые проблемы

Машина Поста. Основные понятия и операции. Финитный 1 – процесс. Способ задания проблемы и формулировка. Алгоритмическая система А.Тьюринга. Машина Тьюринга. Алгоритмическая система Чёрча. Рекурсивные функции. Алгоритмическая система Маркова. Нормальный алгорифм. Ассоциативное исчисление. Алгоритмически неразрешимые проблемы. Проблема соответствий Поста над алфавитом Σ.

Тема 10. Введение в анализ алгоритмов.

Сравнительные оценки алгоритмов. Система обозначений в анализе алгоритмов. Классификация алгоритмов по виду функции трудоёмкости. Асимптотический анализ функций.

Тема 11. Трудоемкость алгоритмов и временные оценки.

Элементарные операции в языке записи алгоритмов. Примеры анализа простых алгоритмов. Переход к временным оценкам. Пример пооперационного временного анализа. Теория сложности вычислений и сложностные классы задач. Теоретический предел трудоемкости задачи. Сложностные классы задач. Проблема P = NP. Примеры NP – полных задач. Пример полного

анализа алгоритма решения задачи о сумме. Формулировка задачи и асимптотическая оценка. Алгоритм точного решения задачи о сумме (метод перебора). Анализ алгоритма точного решения задачи о сумме.

Тема 12. Рекурсивные функции и алгоритмы.

Логарифмические тождества. Методы решения рекурсивных соотношений. Рекурсивные алгоритмы. Основная теорема о рекуррентных соотношениях.

Тема 13. Прямой анализ рекурсивного дерева вызовов.

Алгоритм сортировки слиянием. Слияние отсортированных частей (Merge). Подсчет вершин в дереве рекурсивных вызовов. Анализ трудоемкости алгоритма сортировка слиянием.

Тема 14. Теория и алгоритмы модулярной арифметики

Алгоритм возведения числа в целую степень. Сведения из теории групп. Способы задания дерева. Сведения из теории простых чисел.

Тема 15. Криптосистема RSA и теория алгоритмов

Мультипликативная группа вычетов по модулю n. Степени элементов в Zn^* и поиск больших простых чисел. Криптосистема RSA. Криптостойкость RSA и сложность алгоритмов факторизации.

.

5. Образовательные технологии

Методика преподавания дисциплины **«Математическая логика и теория алгоритмов в программировании»**
и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:
- подготовка к выполнению практических занятий;
- проведение интерактивных лекционных занятий.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 25 % аудиторных занятий. Занятия лекционного типа составляют 50 % от объема аудиторных занятий.

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

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- домашние задания и их защита;
- зачет.

Рубежная проверка знаний в рамках отдельных модулей проводится в форме контроля выполнения практических и домашних заданий. Тематика домашних заданий, соответствует основному содержанию лекционных и практических занятий. Итоговый контроль знаний по дисциплине проводится в форме экзамена в пятом учебном семестре.

Тематика практических занятий

Тема 1. Концептуальный базис математической логики. Построение математической логики. Содержательно и формально построенные логики. Языки логики как реляционные системы. Аксиоматика (система аксиом, система схем аксиом) как подсистема правильно построенных языковых выражений и правила вывода.(2 часа)
Тема 2. Системы счисления. Формальные системы. (2 часа)
Тема 3. Язык логики высказываний. Алфавит логики высказываний. Пропозициональные термы, логические связки и вспомогательные символы. Формулы логики высказываний как формализованный язык. (2 часа)
Тема 4. Логика и исчисление предикатов. Исчисление предикатов как формальная система. Задачи исчисления предикатов. (2 часа)
Тема 5. Основные понятия модальной логики. Синтаксис и семантика модальной логики. Схемы модальных формул. (2 часа)
Тема 6. Немонотонные рассуждения и методы поиска. Стратегии немонотонного вывода в глубину и ширину. (2 часа)
Тема 7. Алгебра логики. Разложение булевых функций по переменным. Классическое представление логических функций: ДНФ, КНФ. Каноническое представление логических функций: СДНФ и СКНФ. Эквивалентные преобразования логических функций.(2 часа)
Тема 8. Алгебра нечетких множеств. Основные понятия и определения. Нечёткие логические формулы. Основные операции над нечёткими множествами и их свойства. (2 часа)
Тема 9. Цели и задачи теории алгоритмов. Практическое применение результатов теории алгоритмов. Формализация понятия алгоритма. Формальные модели, уточняющие понятие алгоритм. Блок-схемы алгоритмов. (2 часа)
Тема 10. Алгоритмические системы Тьюринга, Черча и Маркова. Алгоритмически неразрешимые проблемы. (2 часа)
Тема 11. Сравнительные оценки алгоритмов. Классификация алгоритмов по виду функции трудоёмкости. Асимптотический анализ функций. (2 часа)
Тема 12. Трудоемкость алгоритмов и временные оценки. Пример полного анализа алгоритма решения задачи о сумме. Формулировка задачи и асимптотическая оценка. Алгоритм точного решения задачи о сумме (метод перебора). Анализ алгоритма точного решения задачи о сумме. (2 часа)
Тема 13 Рекурсивные функции и алгоритмы. Логарифмические тождества. Методы решения рекурсивных соотношений. Рекурсивные алгоритмы. Основная теорема о рекуррентных соотношениях. (2 часа)
Тема 14. Прямой анализ рекурсивного дерева вызовов. Алгоритм сортировки слиянием. Слияние отсортированных частей (Merge). Подсчет вершин в дереве рекурсивных вызовов. Анализ трудоемкости алгоритма сортировка слиянием. (2 часа)
Тема 15. Теория и алгоритмы модулярной арифметики. Алгоритм возведения числа в целую степень. (2 часа)
Тема 16. Криптосистема RSA. Криптостойкость RSA и сложность алгоритмов факторизации. (2 часа)
Тема 17. Применение методов математической логики и теории алгоритмов в исследованиях социально-экономических явлений.(2 часа)

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать

ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности

В процессе освоения образовательной программы данная компетенция, в том числе ее отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: - основные понятия и методы математической логики; - элементы математической лингвистики и теории формальных языков; - основные понятия и методы элементов и теории алгоритмов; - основные понятия и термины систем счисления; - основные понятия языка логики; **уметь:** - применять математические методы при решении профессиональных задач повышенной сложности; - применять на практике методы математической логики; - уметь строить логические выражения в языке логики высказываний и изоморфные им графовые модели (в частности, используя дизъюнктивный и конъюнктивный базисы Буля);	Обучающийся не знает теоретических и практических основ математической логики и теории алгоритмов не умеет - применять математические методы при решении профессиональных задач. Не умеет применять на практике методы теории алгоритмов, - решать задачи алгебры логики. Не владеет навыками алгебры логики при решении практических и профессиональных задач, а также - навыками решения задач алгебры логики.	Обучающийся демонстрирует неполное соответствие следующих знаний и умений: теоретические и практические основы математической логики и теории алгоритмов, применение математических методов при решении профессиональных задач. Применение на практике методов теории алгоритмов, решение задач алгебры логики. Не в полной мере владеет навыками алгебры логики при решении практических и профессиональных задач, а также -навыками решения задач алгебры логики.	Обучающийся демонстрирует соответствие следующих знаний и умений: теоретические и практические основы математической логики и теории алгоритмов, применение математических методов при решении профессиональных задач. Применение на практике методов теории алгоритмов, решение задач алгебры логики. Владеет навыками алгебры логики при решении практических и профессиональных задач, а также -навыками решения задач алгебры логики	Обучающийся демонстрирует полное соответствие следующих знаний и умений: теоретические и практические основы математической логики и теории алгоритмов, применение математических методов при решении профессиональных задач. Применение на практике методов теории алгоритмов, решение задач алгебры логики. Владеет навыками алгебры логики при решении практических и профессиональных задач, а также -навыками решения задач алгебры логики

- применять на практике методы теории алгоритмов; - решать задачи алгебры логики; **владеть:** - навыками алгебры логики (пропозициональной и кванторной); - решения научных и практических задач математическими методами при решении профессиональных задач; - навыками решения задач алгебры логики.				

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Перемитина Т.О. Математическая логика и теория алгоритмов [Электронный ресурс]: учебное пособие /— Томск: Томский государственный университет систем управления и радиоэлектроники, 2016. — 132 с.— Режим доступа: http://www.iprbookshop.ru/72121.html
2. Бесценный, И. П. Математическая логика [Электронный ресурс] : учебное пособие / И. П. Бесценный, Е. В. Бесценная. — Электрон. текстовые данные. — Омск : Омский государственный университет им. Ф.М. Достоевского, 2016. — 76 с. — 978-5-7779-2002-7. — Режим доступа: http://www.iprbookshop.ru/59613.html
3. Унучек С. А. Математическая логика [Электронный ресурс] : учебное пособие /. — Саратов: Ай Пи Эр Медиа, 2018. — 239 с.— Режим доступа: http://www.iprbookshop.ru/69312.html.

б) дополнительная литература:

4. Ткаченко С. В., Сысоев А. С. Математическая логика [Электронный ресурс] : учебное пособие / — Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2013. — 99 с. —Режим доступа: http://www.iprbookshop.ru/55105.html
5. Бесценный, И. П. Математическая логика [Электронный ресурс]: учебное пособие / И. П. Бесценный, Е. В. Бесценная. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2016. — 76 с. — Режим доступа: http://www.iprbookshop.ru/59613.html
6. Балюкевич, Э. Л. Математическая логика и теория алгоритмов [Электронный ресурс] : учебное пособие / Э. Л. Балюкевич, Л. Ф. Ковалева. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2009. — 188 с. — 978-5-374-00220-1. — Режим доступа: http://www.iprbookshop.ru/10772.html.

в) программное обеспечение и интернет-ресурсы:

1. Офисные приложения, MicrosoftOffice 2013 (или ниже) - MicrosoftOpenLicense

   Лицензия № 61984042

2. Операционная система Windows 7(или ниже) – MicrosoftOpenLicense.
3. Система компьютерного моделирования машины Тьюринга (тренажер машины Тьюринга).

8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран) – 1 комплект.

Для проведения практических занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *лекции.*

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. Практические занятия проводятся по теоретическим и проблемным вопросам ИБ.

Важным обстоятельством является привлечение внимания студентов к теме практических занятий, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия.

При проведении практического преподаватель выполняет, в основном, функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает полученные результаты, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на лабораторных занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенции;
- оформление материала в соответствии с требованиями.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалистов **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: к.т.н., доцент Алибеков И. Ю.

Программа утверждена на заседании кафедры “Информационная безопасность”
«30» августа 2021 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»



к.т.н., профессор Н.В. Федоров

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»
ОП (профиль): «Безопасность открытых информационных систем»
Форма обучения: очная
Вид профессиональной деятельности: эксплуатационная; проектно-технологическая

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Математическая логика и теория алгоритмов в программировании»

Состав: 1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
Контрольные вопросы
Экзамен

Составители: к.т.н., доцент Алибеков И.Ю.

Москва, 2021 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Проектирование безопасных информационных систем					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности	знать: - основные понятия и методы математической логики; - элементы математической лингвистики и теории формальных языков; - основные понятия и методы элементов и теории алгоритмов; - основные понятия и термины систем счисления; - основные понятия языка логики; уметь: - применять математические методы при решении профессиональных задач повышенной сложности; - применять на практике методы математической логики; - уметь строить логические выражения в языке логики высказываний и изоморфные им графовые модели (в частности, используя дизъюнктивный и конъюнктивный базисы Буля); - применять на практике методы теории алгоритмов; - решать задачи алгебры логики; владеть: - навыками алгебры логики (пропозициональной и кванторной); - решения научных и практических задач математическими методами при решении профессиональных задач; - навыками решения задач алгебры логики.	лекции, самостоятельная работа, практические занятия	**ДЗ, экзамен**	знание теоретических и практических основ математической логики и теории алгоритмов, применение математических методов при решении профессиональных задач. Применение на практике методов теории алгоритмов, решение задач алгебры логики. Владение навыками алгебры логики при решении практических и профессиональных задач, а также -навыками решения задач алгебры логики

Оценочные средства для текущей аттестации

Домашние задания.

5 семестр

1	Упростить формулу $XY \to XY \to XY \to XY$
2	Показать, что $A \to B, B \to C \vdash A \to A$.
3	Показать, что закон тождества выводим как в первой так и во второй аксиоме.
4	Вывести из первой аксиоматики формулу: $\vdash (A \vee A) \to A$.
5	Доказать во второй аксиоматике выводимость: $A \to B, B \to C \vdash A \to (A \to C)$.
6	Доказать, что третья формулу второй аксиоматики выводима из аксиом первой аксиоматики.
7	Докажите равносильность высказывания: $X \to (\overline{XY \vee Z})$ и $\bar{X} \vee \bar{Y}\bar{Z}$.
8	Доказать справедливость заключения $(A \to B), (B \to C) \vdash (A \to C)$
9	Представьте равносильность п.7 в виде логических следствий.
10	Докажите логическое следствие: $(P \to Q)(R \to S)(S\bar{Q} \to \bar{T})\bar{T} \Rightarrow P \vee R$. a) через соответствующую тавтологию; b) с помощью правил вывода.
11	Докажите равносильность высказываний $A \to (\overline{AB} \vee C)$ и $A \vee \bar{B}\bar{C}$.
12	Докажите логические следствия: $(L \to Q)(S \to P)(QP \to R)\bar{R} \Rightarrow \bar{L} \vee \bar{S}$. a) через соответствующую тавтологию b) с помощью правил вывода c) дедуктивным способом
13	Доказать справедливость цепного заключения, т.е. : $(A \to B), (B \to C) \vdash (A \to C)$.
14	Доказать правило перестановки предпосылок $A \to (B \to C) \vdash B \to (A \to C)$.
15	Доказать, что: a. $x \to y = \bar{x} \vee y$; b. $x \sim y = (x \wedge y) \vee (\bar{x} \wedge \bar{y})$;
16	Докажите теорему дедукции т.е. если $A_1, A_2, \cdots, A_n \vdash B$, то $\vDash A_1 \to (A_2 \to (\cdots \to (A_n \to B) \cdots))$
17	Показать, что высказывание "Если внедрить новую технологию, то качество продукции улучшится. При улучшении качества продукции ее сбыт увеличится". Следовательно, "сбыт продукции увеличивается" является тавтологией.
18	Приняв высказывания $A \to B$ и $B \to C$ в качестве посылок, найдите логическое следствие и выразите его в словесной форме. Каким логическим законом можно воспользоваться для получения логического следствия в этом случае?

19	Покажите, что система высказываний $\{X_1, \cdots, X_n\}$ противоречива, если из нее можно вывести в качестве логического следствия противоречие, т.е. тождественно ложную формулу.
20	Записать категорические высказывания всех четырех типов, если определены одноименные предикаты: a. $P(x) = "X -$ изделие" b. $Q(y) = "Y -$ промышленные испытания"
21	Привести категорические высказывания всех четырех типов к такой форме, в которой используются только кванторы одного типа, если определены одноместные предикаты a. $P(\mathrm{x}) =$ "x – блок ЭВМ" b. $Q(\mathrm{x}) =$ "нормально функционирует ".
22	Записать формулы логики предикатов для утверждения: • все студенты, выполнившие задание получили зачет • ни один студент не пропустил экзамен • не все студенты учатся добросовестно • некоторые студенты отслужили в армии • каждый студент изучает или английский, или немецкий, или французский.
23	Записать категорические высказывания всех четырех типов, если определены одноместные предикаты: a. P(x)="X - изделие" b. Q(y)="Y - промышленные испытание"
24	Записать в виде формул логики предикатов определения: • функция f(x), непрерывна на (0,1); • функция f(x), разрывна на (0,1).
25	Запишите формулу логики предикатов для утверждения: "Все студенты, которые выполнили домашнее задание в заданный срок, получили зачет."
26	Записать все четыре типа категорических высказываний, соответствующих каждому из следующих случаев: • S – подмножество Q (т.е. S⊂Q); • S и Q совпадают (S=Q); • Q – подмножество S (Q⊂S); Если одноместные предикаты S(x) и Q(x) являются определяющими свойствами подмножеств S и Q некоторого универсума.
27	Рассматривая одноместные предикаты S(x) и P(x) как определяющие свойства подмножеств S и P некоторого универсума, записать все категорические высказывания четырех типов, которые соответствуют каждому из следующих случаев: • S и P совпадают (S=P); • S и P пересекаются (S∩P≠0); • S и P не пересекаются (S∩P=0).

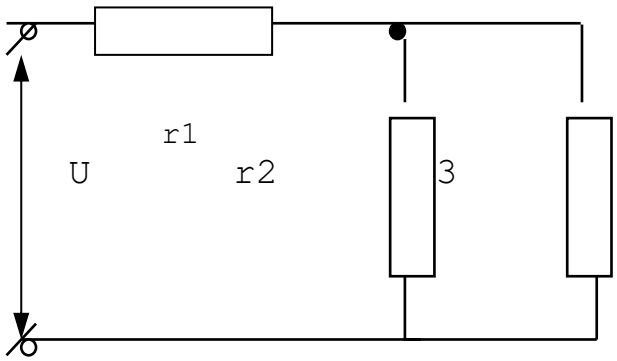
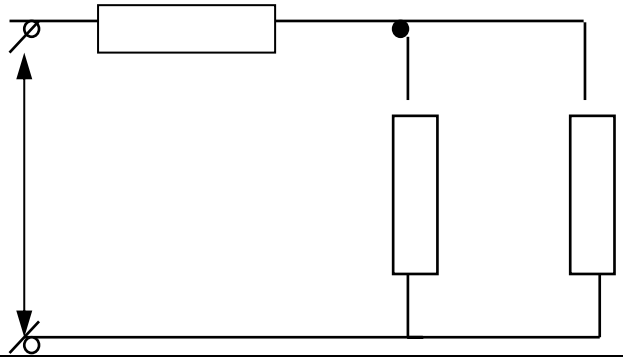
28	Привести категорические высказывания всех четырех типов к такой форме, в которой используются только кванторы одного типа, если определены одноместные предикаты a. P(x) = “x – блок ЭВМ ” b. Q(y) = “y – нормально функционирует ”
29	Записать предикаты, задающие подмножество дуг графа, сходящих из вершины **а**; - подмножество дуг графа, входящих в вершину **в**; - подмножество ребер графа, инцидентных вершине **а**; - подмножество ребер графа, соединяющих вершины **а** и **в**;
30	Запишите предикаты, задающие: a) Подмножество дуг графа, исходящих из вершины a, b) Подмножество вершин графа, инцидентных входящим дугам, c) Подмножество смежных вершин графа.
31	Приведите к предварённой форме формулу: $\forall x\ F_1(x) \to \exists \bar{x}(F_2(y) \vee \forall y\ F_3^2(x,y))$.
32	Приведите к предваренной форме формулу: $\exists x\ F_1(x) \to \overline{\forall x}(F_2(x) \vee \exists y\ F_3^2(x,y))$.
33	Привести к предваренной форме формулу : $\forall x\ F_1(x) \to \overline{\forall x}(F_2(y) \vee \exists y\ F_3^2(x,y))$.
34	Преобразовать следующее высказывание: $\forall x\ (S(x) \to \overline{P(x)})$.
35	Расширить следующую формулу: $\forall x\left(S(x) \to\ \exists y\ \left(Q(y) \wedge R^2(x,y)\right)\right)$, где S(x): x – простое число, Q(y): y – четное число, R(x,y): y делится на x.
36	Записать формулы логики предикатов для утверждений: - все студенты, выполнившие задание, получили зачет; - ни один студент не пропустил экзамен; - не все студенты учатся добросовестно; - некоторые студенты отслужили в армии; каждый студент изучает или английский или немецкий или французский язык.
37	Переведите числа из десятичной системы счисления в двоичную, восьмеричную и шестнадцатеричную системы счисления. а) 948; б) 763; в) 994,125; г) 523,25; д) 203,82.
38	Переведите числа в десятичную систему счисления. а)1110001112; б)1000110112; в)1001100101,10012; г)1001001,0112; д)335,78; е) 14C,A16.
39	Выполните сложение чисел.

	а) 11101010102+101110012; б) 101110102+100101002; в) 111101110,10112+1111011110,12; г) 1153,28+1147,328; д) 40F,416+160,416.
40	Выполните вычитание чисел. а) 10000001002-1010100012; б) 10101111012-1110000102; в) 1101000000,012-1001011010,0112; г) 2023,58-527,48; д) 25E,616-1B1,516.
41	Выполните умножение чисел. а) 10010112*10101102; б) 1650,28*120,28; в) 19,416*2F,816.
42	Что такое алфавит системы счисления?
43	В чем различия позиционных и непозиционных систем счисления?
44	В каким областях применяются системы счисления?
45	Дать определение «логика высказываний»
46	Запишите в символической форме и установите логичность высказывания: «Если перекомпоновать функциональные узлы ЭВС, стоимость его понизится, а если применить другую схемотехническую элементарную базу, повысится надежность ЭВС. Можно или перекомпоновать изделие, или применить новую элементную базу. Однако, если перекомпоновать узлы, то надежность ЭВС не повысится, а если применить другую элементную базу, то не снизится стоимость изделия. Итак, надежность увеличится тогда и только тогда, когда стоимость не снижается».
47	Что лежит в основе алфавита языка логики?
48	Какие формулы называют тождественно истинными в языке логики?
49	Из чего состоит алфавит логики?
50	Какие формулы называют тождественно ложными в языке логики?
51	Какие формулы называют выполненными в языке логики?
52	В симфонический оркестр приняли на работу трёх музыкантов: Брауна, Смита и Вессона, умеющих играть на скрипке, флейте, альте, кларнете, гобое и трубе. Известно, что: 1. Смит самый высокий; 2. играющий на скрипке меньше ростом играющего на флейте; 3. играющие на скрипке и флейте и Браун любят пиццу;

	4. когда между альтистом и трубачом возникает ссора, Смит мирит их; 5. Браун не умеет играть ни на трубе, ни на гобое. На каких инструментах играет каждый из музыкантов, если каждый владеет двумя инструментами?
53	Написать определение алгебры логики.
54	Выписать основные аксиомы алгебры логики
57	По заданной преподавателем таблице истинности логической функции Z = Z(x1, x2, x3) найти ее СДФН и СКФН
58	Упростить формулу при помощи таблицы истинности (рекомендация: использовать СДНФ и СКНФ) и правил де Моргана 1. $z = \overline{\overline{x_1 x_2} + \overline{x_3}}$ 2. $z = \overline{\overline{x_2 x_1 x_3}}$ 3. $z = \overline{x_3}\,\overline{(x_1 + x_2)}$
59	Упростить формулу $(x \vee y)(\overline{xy} \vee z) \vee z \vee (x \vee y)(u \vee v)$
60	Упростить формулу $(xyz) \vee (\overline{xyz}) \vee \overline{x}y$
61	Упростить формулу $x\overline{y}\overline{z} \vee xy\overline{z} \vee \overline{x}yz \vee xyz$
62	Упростить формулу: $(\overline{x}yz) \vee (x\overline{y}z) \vee (xy\overline{z})$
63	Выразите все логические функции двух переменных через штрих Шеффера. Приведите таблицы соответствия.
64	Синтезировать принципиальную схему блока управления индикацией правильности ответов студентов, если: – задаются пять вопросов, требующих установить истинность или ложность определенных утверждений; – экзаменуемый отвечает, нажимая кнопки, соответствующие тем вопросам, на которые хочет дать ответ "истина"; – схема зажигает элемент индикации, соответствующий поставленному вопросу, при нажатии кнопки; – схема индицирует правильное число ответов.
65	На столе лежат в ряд пять монет: средняя — вверх орлом, а остальные — вверх решкой. Разрешается одновременно перевернуть три рядом лежащие монеты. Можно ли при помощи нескольких таких переворачиваний все пять монет положить вверх орлом?
66	В гости пришло 10 гостей и каждый оставил в коридоре пару калош. Все пары калош имеют разные размеры. Гости начали расходиться по одному, одевая любую пару калош, в которые они могли влезть (т.е. каждый гость мог надеть пару калош, не меньшую, чем его собственные). В какой-то момент обнаружилось, что ни один из оставшихся гостей не может найти себе пару калош, чтобы уйти. Какое максимальное число гостей могло остаться?

67	В доме, который был заселён только супружескими парами с детьми, проводилась перепись населения. Человек, проводивший перепись, в отчёте указал: "Взрослых в доме больше, чем детей. У каждого мальчика есть сестра. Мальчиков больше, чем девочек. Бездетных семей нет". Этот отчёт был неверен. Почему?
68	Имеются чашечные весы без гирь и 3 одинаковые по внешнему виду монеты. Одна из монет фальшивая, причём неизвестно, легче она настоящих монет или тяжелее (настоящие монеты одного веса). Сколько надо взвешиваний, чтобы определить фальшивую монету? Решите ту же задачу в случаях, когда имеется 4 монеты и 9 монет.
69	Построить контактные схемы, реализующие функции двух переменных: импликацию, отрицание импликации, эквиваленцию, сумму по модулю два, штрих Шеффера, стрелку Пирса.
70	Приведите к СДНФ и СКНФ формулу: $y = (((x_1 \to x_3)x_2) \to x_3)x_1 \to x_2)$.
71	Найти СДНФ для формул: $x \vee y$; $(\overline{x \vee z})(x \to y)$; $(x \sim y)(\overline{z \to t})$; $x \vee yz$; $xy\bar{x}z \vee xt$; $\overline{xy} \vee yzt \vee \bar{x}yzt$.
72	Дать определение линейного алгоритма. Привести пример.
73	Дать определение разветвляющегося алгоритма. Привести пример.
74	Дать определение циклического алгоритма. Привести пример.
75	Дать определение вспомогательного алгоритма. Привести пример.
76	Составить алгоритм вычисления корней уравнения X^2+B*X+C=0. Оценить сложность алгоритма
77	Составить алгоритм вычисления корней уравнения A*X^2+B*X+C=0. Оценить сложность алгоритма
78	Составить алгоритм для нахождения НОД двух натуральных чисел.
79	Является ли алгоритмически разрешимой следующая задача: Вычислить *n*- ое совершенное число

80	3. Составить алгоритм для нахождения значения функции F(n), где n – целое неотрицательное число, если F(0)=0; F(1)=1; F(2n)=F(n); F(2n+1)=F(n)+F(n+1). 4. Составить алгоритм для нахождения значения sin x с точностью до 0,0001, используя разложение в ряд Маклорена. 5. Доказать, что функция примитивно рекурсивная: f(x)=x!? ((здесь 0!=1) 6. Доказать, что функция примитивно рекурсивная: f(x,y)=min(x,y) 7. Вычислить значение $\mu_{y\angle z}((3^y+ y^2+5)>20)$, при z= 10; 4. 8. Вычислите значение функциb: $N(I_3(1, 2, Z(x)), I_2(Z(x), N(2))$ 9. Какую функцию вычисляет машина Т со следующей программой: $q_1 0 \rightarrow q_2 0 R$, $q_1 1 \rightarrow q_0 1$, $q_2 0 \rightarrow q_0 1$, $q_2 1 \rightarrow q_2 1 R$?
81	10. Является ли алгоритмически разрешимой следующая задача: Найти x такие, что $ax^5+bx^4+cx^3+kx^2+yx+p=0$ 11. Применить операцию примитивной рекурсии к функциям $g(x_1)$ и $h(x_1;x_2;x_3)$ по переменным x_2 и x_3. Функцию $f(x_1;x_2)=R(g,h)$ записать в «аналитической» форме: $g(x_1)= x_1$; $h(x_1;x_2;x_3)= x_1 + x_3$. 12. Вычислить значение функции: $\begin{cases} f(x,0) = x, \\ f(x, y+1) + f(x, y) + x + 3y \end{cases}$ на 6 шаге.
82	Составить формальную и алгоритмическую модели решения задачи. В книжном магазине вы желаете купить три книги. У вас имеется небольшая сумма наличных денег и пластиковая карта, на счету которой большая сумма денег. Вам бы не хотелось сегодня пользоваться пластиковой картой, так как Вы в дальнейшем запланировали крупную покупку. Определите способ покупки.
83	Составить формальную и алгоритмическую модели решения задачи. Определите вариант пути от дома до места учебы, в зависимости от времени выхода из дома и времени начала учебных занятий.
84	Составить формальную и алгоритмическую модели решения задачи. В избирательной компании в органы власти участвуют две партии: зеленых и прозрачных. Какая информация будет опубликована в СМИ по итогам голосования?
85	1. На вопрос, какая завтра будет погода, синоптик ответил: 1. Если не будет ветра, то будет пасмурная погода без дождя. 2. Если будет дождь, то будет пасмурно и без ветра. 3. Если будет пасмурная погода, то будет дождь и не будет ветра. Какая будет погода?
86	Вадим, Сергей и Михаил изучают различные иностранные языки: китайский, японский и арабский. На вопрос, какой язык изучает каждый из них, один ответил: "Вадим изучает китайский, Сергей не изучает китайский, а Михаил не

	изучает арабский". Впоследствии выяснилось, что в этом ответе только одно утверждение верно, а два других ложны. Какой язык изучает каждый из молодых людей?
87	Выполнить формальную постановку задачи. Определить мощность, потребляемую в приведенной ниже электрической цепи (Примечание: любое из сопротивлений может быть равным нулю). 
88	Выполнить формальную постановку задачи. Определить мощность, потребляемую в приведенной ниже электрической цепи (Примечание: проводимость любой из ветвей может быть равна бесконечности). 
89	Составить формальную и алгоритмическую модели решения задачи. Для двух чисел X, Y определить, являются ли они корнями уравнения A*P^4+D*P^2+C=0.
90	Составить алгоритм для ответов на вопросы, возникающие на этапе формального решения задачи.
91	Составить алгоритм для нахождения НОД двух натуральных чисел.
92	Является ли алгоритмически разрешимой следующая задача: Вычислить *n*- ое совершенное число
93	Сколько номеров автомобилей может выдать автоматизированная информационная система ГИБДД, если автомобиль разыскивается только по одной букве и одной цифре его регистрационного кода?
94	Записать с помощью формулы, выделяя более простые высказывания “ДЖО ПОЛУЧИТ ПРИЗ”, “ДЖО УМЕН”, “ДЖИМ ГЛУП” и обозначая их логическими переменными **A**, **B** и **C** соответственно: а) Джо получит приз в том и только в том случае, если Джо умен, а Джим глуп. б) Джо умен и Джо получит приз, а Джим глуп. в) Джо не получит приз, если Джо умен и Джим не глуп. г) Джо не получит приз, если Джо не умен, а Джим не глуп.

95	Является ли формулой следующая запись? (A -> B) -> ((C v D))
96	Каждый ученик в классе изучает либо английский, либо французский язык, либо оба эти языка. Английский язык изучают 25 человек, французский - 27 человек, а то т и другой - 18 человек. Сколько всего учеников в классе?
97	Алеша, Боря и Гриша нашли в земле сосуд. Рассматривая удивительную находку, каждый высказал по 2 предположения: Алеша: «Этот сосуд греческий и изготовлен в V веке». Боря: Этот сосуд финикийский и изготовлен в III веке». Гриша: «Этот сосуд не греческий и изготовлен в IV веке». Учитель истории сказал ребятам, что каждый из них прав только в одном из двух предположений. Где и в каком веке изготовлен сосуд?
98	Является ли формулой следующая запись? (A -> B) -> ((C v D))
99	Каждый ученик в классе изучает либо английский, либо французский язык, либо оба эти языка. Английский язык изучают 25 человек, французский - 27 человек, а то т и другой - 18 человек. Сколько всего учеников в классе?
100	Алеша, Боря и Гриша нашли в земле сосуд. Рассматривая удивительную находку, каждый высказал по 2 предположения:

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена по дисциплине

1. Исчисление высказываний: аксиоматики, способы задания, правило вывода.
2. Отношение логического следования и логической эквивалентности на множестве высказываний.
3. Законы логики высказываний.
4. Исчисление предикатов : аксиоматики и правила выводов.
5. Эквивалентные преобразования кванторной логики.
6. Предикаты. Приведенные и предваренные формы
7. Исторические аспекты разработки теории алгоритмов;
8. Цели и задачи классической теории алгоритмов;
9. Виды систем счисления и представление данных. Операции с числами в системах счисления.
10. Язык алгоритмов. Подходы к математическому уточнению понятия «алгоритм».
11. Блок-схемы алгоритмов.
12. Математическое уточнение понятия «алгоритм» с помощью рекурсивных функций, тезис Черча.
13. Нормальные алгорифмы, принцип нормализации.

14. Формализации алгоритма, определения Колмогорова и Маркова;
15. Требования к алгоритму, связанные с формальными определениями;
16. Понятие общей и конкретной проблемы по Посту;
17. Пространство символов и примитивные операции в машине Поста;
18. Понятие финитного 1-процесса в машине Поста;
19. Способы задания проблем и формулировка 1;
20. Гипотеза Поста;
21. Формальное описание машины Тьюринга;
22. Функция переходов в машине Тьюринга;
23. Понятие об алгоритмически неразрешимых проблемах
24. Проблема позиционирования в машине Поста;
25. Проблема соответствий Поста над алфавитом Σ;
26. Проблема останова в машине Тьюринга;
27. Проблема эквивалентности и тотальности;
28. Формальная система языка высокого уровня;
29. Понятие трудоемкости алгоритма в формальном базисе;
30. Обобщенный критерий оценки качества алгоритма,
31. Обозначения в анализе алгоритмов: худший, лучший и средний случаи;
32. Классификация алгоритмов по виду функции трудоемкости;
33. Примеры количественных и параметрически–зависимых алгоритмов;
34. Обозначения в асимптотическом анализе функций;
35. Примеры функций, не связанных асимптотическими обозначениями;
36. Элементарные операции в псевдоязыке высокого уровня;
37. Анализ трудоемкости основных алгоритмических конструкций;
38. Построение функции трудоемкости для задачи суммирования матрицы;
39. Построение функции трудоемкости для поиска максимума в массиве;
40. Проблемы при переходе от трудоемкости к временным оценкам;
41. Методики перехода от функции трудоемкости к временным оценкам;
42. Возможности пооперационного анализа алгоритмов на примере задачи умножения комплексных чисел;
43. Теоретический предел трудоемкости задачи;
44. Основные задачи теории сложности вычислений
45. Понятие сложностных классов задач, класс P;
46. Сложностной класс NP, понятие сертификата;
47. Проблема P=NP, и ее современное состояние;
48. Сводимость языков и определение класса NPC;
49. Примеры NP – полных задач;
50. Задача о клике и ее особенности;
51. Формулировка задачи о сумме;
52. Асимптотическая оценка сложности алгоритма для прямого перебора;
53. Алгоритм решения задачи о сумме;
54. Алгоритм увеличения на единицу двоичного счетчика;
55. Оценки трудоемкости для лучшего и худшего случая;

56. Функция трудоемкости алгоритма для решения задачи о сумме;
57. Понятие индукции и рекурсии;
58. Примеры рекурсивного задания функций;
59. Рекурсивная реализация алгоритмов
60. Трудоемкость механизма вызова функции в языке высокого уровня;
61. Рекурсивное дерево, рекурсивные вызовы и возвраты;
62. Трудоемкость рекурсивного алгоритма вычисления факториала;
63. Анализ рекурсивных соотношений методом итераций;
64. Анализ рекурсивных соотношений методом подстановки;
65. Общий вид функции трудоемкости при решении задач методом декомпозиции;
66. Основная теорема о рекуррентных соотношениях;
67. Примеры решения рекуррентных соотношений на основе теоремы Бентли – Хакен – Сакса;
68. Рекурсивный алгоритм сортировки слиянием
69. Процедура слияния двух отсортированных массивов
70. Оценка трудоемкости процедуры слияния;
71. Подсчет вершин в дереве рекурсивных вызовов для алгоритма сортировки слиянием;
72. Анализ алгоритма рекурсивной сортировки методом прямого подсчета вершин рекурсивного дерева;
73. Функции подсчета количества битов и количества единиц в двоичном представлении числа и их свойства;
74. Алгоритм быстрого возведения в степень
75. Анализ трудоемкости алгоритма быстрого возведения в степень;
76. Понятие полугруппы, моноида и группы, примеры групп;
77. Сравнения и сведения из теории простых чисел;
78. Мультипликативная группа вычетов по модулю N и ее свойства;
79. Степени элементов группы и теорема Ферма-Эйлера;
80. Вероятностный тест Миллера-Рабина для поиска простых чисел;
81. Криптосистема RSA;
82. Применение теории алгоритмов к анализу криптостойкости RSA.

Пример билета.

1. Общий вид функции трудоемкости при решении задач методом декомпозиции;
2. Формальное описание машины Тьюринга;
3. Упростить формулу $(x \vee y)(\overline{xy} \vee z) \vee z \vee (x \vee y)(u \vee v)$

Структура и содержание дисциплины «Математическая логика и теория алгоритмов в программировании»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	Лаб	П/С	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	Пятый семестр														
1.1	Введение. Роль математической логики и теории алгоритмов в прикладных науках. Историческая справка. Предмет, цель и содержание курса «Математическая логика и теория алгоритмов в программировании». Основные понятия и определения алгебры логики и теории алгоритмов. Концептуальный базис математической логики. Построение математической логики. Содержательно и формально построенные логики. Языки логики как реляционные системы.	1	1	2			4								
1.2	Понятие системы счисления. Позиционные системы счисления. Примеры перевода чисел из одной системы счисления в другую. Алфавит как множество дескриптивных, логических и вспомогательных символов. Синтаксис языковых выражений. Аксиоматика (система аксиом, система схем аксиом) как подсистема правильно построенных языковых выражений и правила вывода. Исчисления. Примеры	1	2	2		2	4								

	исчисления высказываний и исчисления предикатов.														
1.3	Краткий экскурс в историю логики высказываний. Логика и исчисление высказываний. Классическое определение исчисления высказываний. Конструктивное определение исчисления высказываний. Язык логики высказываний. Алфавит логики высказываний. Пропозициональные термы, логические связки и вспомогательные символы. Формулы логики высказываний как формализованный язык. Кванторная алгебра логики. Субъектно-предикатная структура простых высказываний. Предикаты. Кванторы и квантификация предикаторных формул. Представление кванторов логическими связками на конечном универсуме рассмотрения. Свойства кванторов. Правила эквивалентных преобразований формул кванторной логики.	1	3	2		2	4								
1.4	Язык логики предикатов. Дескриптивные символы: индивидные константы, логические связки, предметно-функциональные и предметно-предикаторные константы. Синтаксис языка логики предикатов. Языковые выражения – термы и формулы. Семантики языка логики предикатов. Модель интерпретации. Интерпретирующая функция. Логика и исчисление предикатов. Исчисление предикатов как формальная система. Задачи исчисления предикатов. Отношения логического следования и логической эквивалентности. Примеры	1	4	2		2	4								

	аксиоматик и правил вывода классической логики предикатов. Правила вывода в логике предикатов первого порядка. Методы вывода в классическом исчислении предикатов.														
1.5	Основные понятия модальной логики. Синтаксис и семантика модальной логики. Схемы модальных формул. Бинарные отношения. Обзор других формально-логических моделей.	1	5	2			4								
1.6	Модифицируемые рассуждения и свойства немонотонных логик. Зацикливание немонотонных рассуждений и его преодоление. Стратегии немонотонного вывода в глубину и ширину.	1	6	2		4	4				+				
1.7	Булева алгебра логики. Язык алгебры логики. Задача Венна. Логические (булевы) функции как n-арные операции. Способы задания логических функций. Табличные задания булевых функций. Существенные и несущественные переменные. Равенство булевых функций. Эквивалентность. Разложение булевых функций по переменным. Классическое представление логических функций: ДНФ, КНФ. Каноническое представление логических функций: совершенная дизъюнктивная нормальная форма (СДНФ), совершенная конъюктивная нормальная форма (СКНФ). Эквивалентные преобразования логических функций.	1	7	2		4	4								
1.8	Алгебра множеств (алгебра Кантора). Упорядоченные, частично упорядоченные множества. Алгебра нечетких множеств. Основные понятия и определения. Нечёткие	1	8	2		2	4								

	логические формулы. Основные операции над нечёткими множествами и их свойства														
1.9	Цели и задачи теории алгоритмов. Практическое применение результатов теории алгоритмов. Формализация понятия алгоритма. Формальные модели, уточняющие понятие алгоритм. Блок-схемы алгоритмов.	1	9	2		4	4								
1.10	Машина Поста. Основные понятия и операции. Финитный 1 – процесс. Способ задания проблемы и формулировка. Алгоритмическая система А.Тьюринга. Машина Тьюринга. Алгоритмическая система Чёрча. Рекурсивные функции. Алгоритмическая система Маркова. Нормальный алгорифм. Ассоциативное исчисление. Алгоритмически неразрешимые проблемы. Проблема соответствий Поста над алфавитом Σ.	1	10	2		2	4				+				
1.11	Сравнительные оценки алгоритмов. Система обозначений в анализе алгоритмов. Классификация алгоритмов по виду функции трудоёмкости. Асимптотический анализ функций.	5	11	2		2	4								
1.12	Элементарные операции в языке записи алгоритмов. Примеры анализа простых алгоритмов. Переход к временным оценкам. Пример пооперационного временного анализа. Раскраска графов. Теория сложности вычислений и сложностные классы задач. Теоретический предел трудоемкости задачи. Сложностные классы задач. Проблема P = NP. Примеры NP – полных задач. Пример полного анализа алгоритма решения задачи о сумме.	1	12	2		2	4				+				

	Формулировка задачи и асимптотическая оценка. Алгоритм точного решения задачи о сумме (метод перебора). Анализ алгоритма точного решения задачи о сумме.														
1.13	Логарифмические тождества. Методы решения рекурсивных соотношений. Рекурсивные алгоритмы. Основная теорема о рекуррентных соотношениях.	1	13	2		2	6								
1.14	Алгоритм сортировки слиянием. Слияние отсортированных частей (Merge). Подсчет вершин в дереве рекурсивных вызовов. Анализ трудоемкости алгоритма сортировка слиянием.	1	14	2		4	6				+				
1.15	Алгоритм возведения числа в целую степень. Сведения из теории групп. Способы задания дерева. Сведения из теории простых чисел.	1	15	2		2	6								
1.16	Мультипликативная группа вычетов по модулю n. Степени элементов в Z_n^* и поиск больших простых чисел. Криптосистема RSA. Криптостойкость RSA и сложность алгоритмов факторизации.	1	16	2		2	6				+				
1.17	Заключение. Применение методов математической логики и теории алгоритмов в исследованиях социально-экономических явлений.	1	17-18	4											
	Форма аттестации													Э	
	Всего часов по дисциплине			36		36	72								