МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук
(наименование факультета/института/САЕ)

КАТАЛОГ АННОТАЦИЙ ДИСЦИПЛИН

Основной профессиональной образовательной программы

АНАЛИЗ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ
(наименования направленностей (профилей) подготовки)

по направлению подготовки

10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
(указывается код и наименование направления подготовки)

Томск-2020

Содержание

Б1.Б.1.01 История ... 4
Б1.Б.1.02 Философия ... 6
Б1.Б.1.03 Иностранный язык ... 8
Б1.Б.1.04 Безопасность жизнедеятельности ... 17
Б1.Б.1.05 Физическая культура и спорт ... 19
Б1.Б.1.06 Основы информационной безопасности ... 21
Б1.Б.1.07 Языки программирования ... 23
Б1.Б.1.08 Операционные системы ... 27
Б1.Б.1.09 Системы управления базами данных ... 30
Б1.Б.1.10 Электроника и схемотехника ... 32
Б1.Б.1.11 Организационное и правовое обеспечение информационной безопасности ... 34
Б1.Б.1.12 Техническая защита информации ... 38
Б1.Б.1.13 Модели безопасности компьютерных систем ... 40
Б1.Б.1.14 Криптографические методы защиты информации ... 43
Б1.Б.1.15 Криптографические протоколы ... 46
Б1.Б.1.16 Экономика ... 49
Б1.Б.1.17 Правоведение ... 51
Б1.Б.1.18 Основы управленческой деятельности ... 53
Б1.Б.1.19 Социальная инженерия ... 55
Б1.Б.1.20 Психология ... 57
Б1.Б.1.21 Математический анализ ... 59
Б1.Б.1.22 Геометрия ... 62
Б1.Б.1.23 Теория вероятностей и математическая статистика ... 64
Б1.Б.1.24 Алгебра ... 67
Б1.Б.1.25 Математическая логика и теория алгоритмов ... 72
Б1.Б.1.26 Дискретная математика ... 74
Б1.Б.1.27 Дискретная математика. Теория автоматов ... 77
Б1.Б.1.28 Теория информации ... 80
Б1.Б.1.29 Физика ... 82
Б1.Б.1.30 Информатика ... 85
Б1.Б.1.31 Алгоритмы и структуры данных I ... 88
Б1.Б.1.32 Аппаратные средства вычислительной техники ... 90
Б1.Б.1.33 Компьютерные сети ... 92
Б1.Б.1.34 Защита в операционных системах ... 94
Б1.Б.1.35 Основы построения защищённых компьютерных сетей ... 96
Б1.Б.1.36 Основы построения защищённых баз данных ... 99
Б1.Б.1.37 Защита программ и данных ... 101

Б1.Б.1.38 Теоретико-числовые методы в криптографии ... 103
Б1.Б.1.39 Сети и системы передачи информации ... 106
Б1.Б.1.40 Аппаратная реализация криптоалгоритмов ... 109
Б1.Б.1.41 Алгоритмы и структуры данных II ... 112
Б1.Б.2.01 Методы верификации ... 115
Б1.Б.2.02 Безопасность веб-приложений ... 117
Б1.Б.2.03 Алгоритмы кодирования и сжатия информации ... 119
Б1.Б.2.04 Теория кодирования, сжатия и восстановления информации ... 122
Б1.Б.2.05 Анализ уязвимостей программного обеспечения ... 124
Б1.В.01 Элективные дисциплины по физической культуре и спорту ... 126
Б1.В.02 Теория чисел ... 127
Б1.В.03 Введение в математику ... 129
Б1.В.04 Комбинаторика ... 131
Б1.В.05 Булевы функции в криптографии ... 133
Б1.В.06 Профессиональный перевод специальной литературы ... 135
Б1.В.07 Методы компиляции ... 138
Б1.В.08 Введение в специальность 1 ... 140
Б1.В.09 Введение в специальность 2 ... 142
Б1.В.ДВ.01.01 Теория вычислительной сложности ... 144
Б1.В.ДВ.01.02 Алгоритмические системы ... 146
Б1.В.ДВ.02.01 Квантовые вычисления ... 148
Б1.В.ДВ.02.02 Алгебраические системы ... 150
Б1.В.ДВ.03.01 Облачные вычисления ... 152
Б1.В.ДВ.03.02 Постквантовая криптография ... 154
Б1.В.ДВ.04.01 Технология разработки программ ... 156
Б1.В.ДВ.04.02 Промышленное программирование ... 158
Б1.В.ДВ.05.01 Спецсеминар АБКС ... 160
Б1.В.ДВ.05.02 Спецсеминар ММЗИ ... 162
ФТД.01 Технология блокчейн ... 164
ФТД.02 СУБД Oracle ... 166

Б1.Б.1.01 История
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	Специалитет	1 курс 1 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Морев Владимир Алексеевич, канд. ист. наук, доцент	Факультет исторических и политических наук, кафедра истории и документоведения

Пререквизиты	Параллельно осваиваемые дисциплины
	Иностранный язык

Цель и задачи дисциплины

Цель дисциплины – научить студента использовать полученные исторические знания о человеке, обществе, культуре в учебной и профессиональной деятельности.
Задачи дисциплины: изучение эпох мировых цивилизаций, современной картины мира, анализ исторической информации в различных источниках.

Результаты обучения	Методы обучения	Методы оценивания
Демонстрирует понимание исторической обусловленности межкультурного разнообразия общества. Находит и использует необходимую для саморазвития и взаимодействия с другими информацию о культурных особенностях и традициях различных социальных групп. Демонстрирует уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения.	• Семинары • Лекции	• Тесты • Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
1. Теория и методология исторической науки	1	2				2	Изучение теоретического материала по теме 1.
2. Древняя Русь и социально-политические изменения в русских землях в XIII – сер. XV в	1	2				2	Изучение теоретического материала по теме 2.
3. Образование и развитие Московского государства (вторая половина XV – XVI в.)	1	3				2	Изучение теоретического материала по теме 3.

4. Дальнейшее развитие Московского государства в XVII в.	1	3				2	Изучение теоретического материала по теме 4.
5. Российская империя в XVIII – первой пол. XIX в.	2	3				2	Изучение теоретического материала по теме 5.
6. Российская империя во второй пол. XIX – начале XX в.	2	3				3	Изучение теоретического материала по теме 6.
7. Россия в условиях войн и революций (1914 – 1922 гг.)	2	3				3	Изучение теоретического материала по теме 7.
8. СССР в 1922 – 1930-е гг.	2	3				3	Изучение теоретического материала по теме 8.
9. Вторая мировая война (1939 – 1945 гг.) и Великая Отечественная война (1941 – 1945 гг.)	2	3				3	Изучение теоретического материала по теме 9.
10. СССР в послевоенный период (1945 – 1953 гг.)	2	3				3	Изучение теоретического материала по теме 10.
11. СССР в 1953 – 1991 гг.	2	3				3	Изучение теоретического материала по теме 11.
12. Становление новой российской государственности и новой экономической системы (1992 – 2000-е гг.)	2	3				5,3	Изучение теоретического материала по теме 12.
Подготовка к промежуточной аттестации				2,7		15,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего:	20	34		4,7	0,3	49,0	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Практические работы	48%	В течение семестра	**Отлично**: сдано более 85% практических заданий; **Хорошо**: сдано более 65% практических заданий; **Удовлетворительно**: сдано более 35% практических заданий.
Экзамен	52%	В конце семестра	**Должны быть сданы обязательные практические задания, иначе оценка "Неудовлетворительно".** **Отлично**: студент полностью владеет теоретическим материалом; **Хорошо**: студент полностью владеет теоретическим материалом, но допускает ошибки или неточности; **Удовлетворительно**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает грубые ошибки; **Неудовлетворительно**: студент не сдал все лабораторные работы и/или не освоил большую часть теоретического материала.

Литература
Вдовин А.И. История СССР от Ленина до Горбачёва – М.: Вече, 2014. Чураков Д. О., Вдовин А. И., Барсенков А. С. История России XX – начала XXI века Т. 2. – М.: Юрайт, 2016.
Дополнительные рекомендации к дисциплине
Алишина Г. Н. Отечественная история – Томск: Томский государственный университет, 2010.

Б1.Б.1.02 Философия
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	Специалитет	1 курс 2 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Фаненштиль Татьяна Владимировна, канд. филос. наук, доцент	Философский факультет, кафедра философии и методологии науки

Пререквизиты	Параллельно осваиваемые дисциплины
История	Экономика

Цель и задачи дисциплины

Цель дисциплины – формирование высокого уровня философской культуры и рационального мышления будущего специалиста, правильного понимания сущности современных мировоззренческих проблем, их источников и теоретических вариантов решения, а также принципов и идеалов, определяющих цели, средства и характер деятельности людей.

Задачи дисциплины: формирование научных основ мировоззрения студентов, умения осуществлять логический, методологический и философский анализ развития и функционирования различных сфер жизни общества, в том числе, профессиональной деятельности будущих специалистов.

Результаты обучения	Методы обучения	Методы оценивания
Демонстрирует понимание исторической обусловленности межкультурного разнообразия общества. Находит и использует необходимую для саморазвития и взаимодействия с другими информацию о культурных особенностях и традициях различных социальных групп. Демонстрирует уважительное отношение к историческому наследию и социокультурным традициям различных социальных групп, опирающееся на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и культурных традиций мира (в зависимости от среды и задач образования), включая мировые религии, философские и этические учения.	• Лекции • Семинары	• Тесты • Реферат • Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
1. Мировоззрение и философия	1	1				2	Изучение теоретического материала по теме 1.
2. Предметное самоопределение философии	1	1				2	Изучение теоретического материала по теме 2.
3. Философия в древней Индии и в Древнем Китае	1	2				2	Изучение теоретического материала по теме 3. Подготовка реферата.
4. Философия Древней Греции и Рима	1	2				2	Изучение теоретического материала 4. Подготовка реферата.
5. Философия Средних веков в странах Востока и Европе	1	2				2	Изучение теоретического материала 5. Подготовка реферата.

6. Философия эпохи Возрождения механизмы выдвижения в лидеры	1	2				2	Изучение теоретического материала 6.
7. Философия Нового времени	1	2				2	Изучение теоретического материала 7.
8. Философия эпохи Просвещения	1	2				2	Изучение теоретического материала 8.
9. Немецкая классическая философия	1	2				2	Изучение теоретического материала 9.
10. Русская философия	1	2				2	Изучение теоретического материала 10.
11. Современная Западная философия	1	2				3	Изучение теоретического материала 11.
12. Онтология	1	2				3	Изучение теоретического материала 12.
13. Гносеология	1	2				3	Изучение теоретического материала 13.
14. Аксиология	1	2				3	Изучение теоретического материала 14.
15. Праксиология	1	2				3	Изучение теоретического материала 15.
16. Философская антропология	1	2				3	Изучение теоретического материала 16.
17. Социальная философия	1	2				3	Изучение теоретического материала 17.
18. Глобальные проблемы современности	1	2				3,4	Изучение теоретического материала 18.
Подготовка к промежуточной аттестации				2,6		6,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего:	18	34		4,6	0,3	51,1	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Практические работы	48%	В течение семестра	**Отлично**: сдано более 85% практических заданий; **Хорошо**: сдано более 65% практических заданий; **Удовлетворительно**: сдано более 35% практических заданий.
Экзамен	52%	В конце семестра	**Должны быть сданы обязательные практические задания, иначе оценка "Неудовлетворительно".** **Отлично**: студент полностью владеет теоретическим материалом; **Хорошо**: студент полностью владеет теоретическим материалом, но допускает ошибки или неточности; **Удовлетворительно**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает грубые ошибки; **Неудовлетворительно**: студент не сдал все лабораторные работы и/или не освоил большую часть теоретического материала.

Литература

Алексеев П. В. Философия. - Моск. гос. ун-т им. М. В. Ломоносова, 2015.
Балашов Л. Е. Философия - Дашков и К°, 2013.

Дополнительные рекомендации к дисциплине

Степин В. С. Новая философская энциклопедия. - Мысль, 2010.

Б1.Б.1.03 Иностранный язык
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
10 з.е.	специалитет	1 курс 1, 2 семестр 2 курс 3, 4 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Бутузова Татьяна Владимировна, ст. преподаватель	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Для изучения дисциплины необходимы компетенции, сформированные в результате обучения в средней общеобразовательной школе. Организация обучения дисциплине предполагает обязательное проведение тестирования, охватывающего все виды деятельности (по типу Oxford Placement Test). По результатам тестирования формируются две подгруппы: начинающая и продолжающая.	

Цель и задачи дисциплины

Цель: Целью освоения дисциплины является формирование базового уровня владения иностранным языком, а также формирование межкультурной коммуникативной компетенции для решения социально-коммуникативных задач в профессиональной и научной деятельности при общении с зарубежными партнерами, а также для дальнейшего самообразования.

Задачи:

Знать: нормы, правила и способы осуществления коммуникации в устной и письменной форме на русском и иностранном языках в бытовой и профессиональной сферах межличностного и межкультурного взаимодействия

Уметь: логически верно, аргументировано и ясно строить устную и письменную речь на русском и иностранном языках в бытовой и профессиональной сферах межличностного и межкультурного взаимодействия

Владеть: навыками осуществления коммуникации в устной и письменной форме на русском и иностранном языках в бытовой и профессиональной сферах межличностного и межкультурного взаимодействия.

Результаты обучения	Методы обучения	Методы оценивания
ОК-7 "Способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности"	• Практические занятия • Самостоятельная работа • Групповая работа	• Презентация • Тест • Экзамен/зачет

Содержание дисциплины							
Темы занятий	**Контактные часы**					**Самостоятельная работа**	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен/Зачет/ Зачет с оценкой	Часы СРС	Задания
1 семестр							
Тема 1 **Еда. Влияние еды на нашу физическую и умственную активность.**		6				2	Изучение учебного материала. Подготовка к практическим занятиям Творческое задание (снять видео)
Тема2 **Моя семья. Семейные традиции. Взаимоотношения в семье.**		6				2	Изучение учебного материала. Подготовка к практическим занятиям
Тема 3 **Умете ли вы распоряжаться деньгами? Вы экономны? Или вы транжира?**		6				2	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
Тема4 **Перемены в жизни**		6				2	Изучение учебного материала. Подготовка к практическим занятиям
Тема 5 **Передвижение по городу. (Транспорт)**		6				2	Изучение учебного материала. Подготовка к практическим занятиям Творческое задание (интервью)
Тема 6. **Успехи и неудачи**		6				2	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
Тема 7 **Правила поведения/манеры**		6				2	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
Тема 8 **Спорт. Здоровый образ жизни.**		6				2	Изучение учебного материала. Подготовка к практическим занятиям Творческое задание (снять видео)
Тема 9 **Любовь с первого взгляда** **Грамматика**:		6				2	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
							Подготовка к сдаче зачета
Промежуточный контроль (зачет)							
Итого		54		2,95		15,05	
2 семестр							
Тема 10 **Кино**		6				2	Изучение учебного материала. Подготовка к практическим занятиям Творческое письменное задание (рецензия)
Тема 11 **Первое впечатление**		6				2	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
Тема 12 **Обучение в школе/ВУЗе**		6				2	Изучение учебного материала. Подготовка к практическим занятиям

							Презентация «Старейшие российские и зарубежные ВУЗЫ»
Тема 13 Дом моей мечты		6				2	Изучение учебного материала. Подготовка к практическим занятиям Презентация «Дом моей мечты»
Тема 14 Интернет продажи		6				2	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
Тема 15 Правильно выбранная работа		6				2	Изучение учебного материала. Подготовка к практическим занятиям Творческое письменное задание (резюме)
Тема 16 “Иконы” нашего времени		6				2	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
Тема 17 Удачливые люди		2				2	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
						2	Подготовка к сдаче зачета
Промежуточный контроль (дифференцированный зачет)							
Итого		54		2,95		15,05	
3 семестр							
Компьютеры в нашей жизни Тема1.Использование компьютеров в бытовой и профессиональной сферах жизни человека		6				8	Изучение учебного материала. Подготовка к практическим занятиям Подготовка доклада, сообщения, презентации
Тема2. Конфигурация компьютера. Типы компьютерных систем.		6				8	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
Тема3. Устройства входа/выхода и сохранения информации.		6				8	Изучение учебного материала. Подготовка к практическим занятиям Беседа по заданной теме
Тема4. Устройства для людей с физическими ограничениями.		6				8	Изучение учебного материала. Подготовка к практическим занятиям Презентация «Устройства для людей с физическими ограничениями»
Тема5. Эргономика.		6				8	Изучение учебного материала. Подготовка к практическим занятиям Описать свое рабочее место
Тема 6. Компьютерная безопасность Операционные системы		6				8	Изучение учебного материала. Подготовка к практическим занятиям Подготовка доклада, сообщения, презентации
						4	Подготовка к сдаче зачета
Промежуточный контроль (зачет)							
Итого		54		2,95		51,05	
4 семестр							
Тема7. Компьютерная безопасность		6					Изучение учебного материала. Подготовка к практическим занятиям Подготовка доклада, сообщения, презентации
Тема 8. Программный дизайн.		6				10	Изучение учебного материала.

							Подготовка к практическим занятиям Подготовка доклада, сообщения, презентации
Тема9. Языки программирования		6				10	Изучение учебного материала. Подготовка к практическим занятиям Подготовка доклада, сообщения, презентации
Тема10. Работа в сфере информационных технологий		6				10	Изучение учебного материала. Подготовка к практическим занятиям Подготовка доклада, сообщения, презентации
Тема 11. Социальные сети		6				10	Изучение учебного материала. Подготовка к практическим занятиям Подготовка доклада, сообщения, презентации
Тема 11. ИТ тренды		8				10	Изучение учебного материала. Подготовка к практическим занятиям Презентация новых трендов
Тема 12. Мобильные устройства		6				10	Изучение учебного материала. Подготовка к практическим занятиям Подготовка доклада, сообщения, презентации
						4	Подготовка к устному экзамену
						43,8	
Индивидуальные консультации по дисциплине				2,2			
Прохождение промежуточной аттестации в форме экзамена				2	0,3	15,7	
Итого		44		4,2	0,3	59,5	
Всего		206		13,05	0,3	140,65	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Эссе		В течение семестра	**Эссе** оценивается по 3 основным критериям, каждый из которых может быть оценен по 3 балльной шкале (1-3). Критерий 1 «Решение коммуникативной задачи» **3 балла** – коммуникативная задача выполнена полностью: содержание полно, точно и развёрнуто отражает все аспекты, указанные в задании. Количество слов – 150-200 слов; **2 балла** – коммуникативная задача выполнена частично: один аспект не раскрыт (остальные раскрыты полно), ИЛИ один-два аспекта раскрыты неполно. Количество слов – 150-180 слов; **1 балла –** коммуникативная задача выполнена не полностью: два аспекта не раскрыты (остальные раскрыты полно), ИЛИ все аспекты раскрыты неполно. Количество слов – меньше 120 слов Критерий «Организация высказывания» **3 балла** – высказывание логично и имеет завершённый характер; имеются вступительная и заключительная фразы, соответствующие теме. Средства логической связи используются правильно; **2 балла –** высказывание в основном логично и имеет достаточно завершённый характер, НО отсутствует вступительная или заключительная фраза И/ИЛИ средства логической связи используются недостаточно; **1 балл –** высказывание нелогично И/ИЛИ не имеет

			завершенного характера, вступительная и заключительная фразы отсутствуют, средства логической связи практически не используются. **Критерий 3** «Языковое оформление высказывания» **3 балла** – используемый словарный запас, грамматические структуры соответствуют поставленной задаче (допускается не более двух негрубых лексико-грамматических ошибок; **2 балла –** используемый словарный запас, грамматические структуры соответствуют поставленной задаче (допускается не более четырёх лексико-грамматических ошибок (из них не более двух грубых) **1 балл –** понимание высказывания затруднено из-за многочисленных лексико-грамматических (пять и более лексико-грамматических ошибок. Удельный вес беседы составляет сумму баллов по всем трём критериям
Презентация	10%		**Презентация** оценивается по 4 основным критериям, каждый из которых может быть оценен по 4 балльной шкале (5-2). Критерий 1 «Решение коммуникативной задачи **5 баллов** – содержание презентации соответствует цели, отражает полно и точно все аспекты, указанные в задании; стилевое оформление речи выбрано правильно (допускается 1 нарушение нейтрального стиля); **4 балла** – содержание презентации в основном соответствует цели, задание выполнено в основном: но 1–2 аспекта содержания, указанные в задании, раскрыты не полностью или неточно; стилевое оформление речи в основном правильно (допускается 2–3 нарушения нейтрального стиля); **3 балла** – содержание презентации частично соответствует цели; задание выполнено не полностью: в содержании не раскрыты 1–2 аспекта, ИЛИ 3–4 аспекта содержания раскрыты неполно или неточно, ИЛИ 1 аспект не раскрыт, и 1–2 аспекта содержания раскрыты неполно или неточно; имеются ошибки в стилевом оформлении речи (допускается 4 нарушения нейтрального стиля); **2 балла** – задание не выполнено: все случаи, не указанные в оценивании на 1, 2 и 3 балла, ИЛИ ответ не соответствует требуемому объёму, ИЛИ более 30% ответа имеет непродуктивный характер (т.е. текстуально совпадает с опубликованным источником). Критерий 2 «Организация текста» **5 баллов** – высказывание логично; средства логической связи использованы правильно, структура текста соответствует предложенному плану; **4 балла** – высказывание в основном логично (имеется 1–2 логические ошибки), И/ИЛИ имеется 1–2 недостатка при использовании средств логической связи, И/ИЛИ отсутствуют 1-2 необходимых элементов презентации; **3 балла** – в высказывании имеется 3–4 логические ошибки, И/ИЛИ имеется 3–4 ошибки в использовании средств логической связи, И/ИЛИ отсутствуют 3-4 необходимых элементов презентации; **2 балла** – в высказывании имеется 5 и более логических ошибок И/ИЛИ имеется 5 и более ошибок в использовании средств логической связи, И/ИЛИ отсутствуют 5 и более необходимых элементов

Зачет		В конце семестра	презентации Критерий 3 «Лексический ресурс» **5 баллов** – используемый словарный запас соответствует высокому уровню сложности задания, практически нет нарушений в использовании лексики (допускается 1 лексическая ошибка); **4 балла –** используемый словарный запас соответствует высокому уровню сложности задания, однако имеется 2–3 лексические ошибки, ИЛИ словарный запас ограничен, но лексика использована правильно; **3 балла –** используемый словарный запас не вполне соответствует высокому уровню сложности задания, в тексте имеется 4 лексические ошибки; **2 балла** – используемый словарный запас не соответствует высокому уровню сложности задания, в тексте имеется 5 и более лексических ошибок. Критерий 4 «Грамматический ресурс» **5 баллов –** используемые грамматические средства соответствуют высокому уровню сложности задания, нарушений практически нет (допускается 1–2 не повторяющиеся грамматические ошибки); **4 балла –** используемые грамматические средства соответствуют высокому уровню сложности задания, однако в тексте имеется 3–4 грамматические ошибки; **3 балла –** используемые грамматические средства не вполне соответствуют высокому уровню сложности задания, в тексте имеется 5–7 грамматических ошибок; **2 балла –** используемые грамматические средства не соответствуют высокому уровню сложности задания, имеется 8 и более грамматических ошибок. Удельный вес презентации составляет сумму баллов по всем четырём критериям, поделённую пополам. Например, если итоговая оценка за участие в конференции – 17 баллов, то удельный вес этого задания 8,5. Максимально – 10%. **Беседа по темам** оценивается по 3 основным критериям, каждый из которых может быть оценен по 4 балльной шкале (1-4). Критерий 1 «Решение коммуникативной задачи» **4 балла** – коммуникативная задача выполнена полностью: содержание полно, точно и развёрнуто отражает все аспекты, указанные в задании. Продолжительность высказывания – 10-12 фраз; **3 балла** – коммуникативная задача выполнена частично: один аспект не раскрыт (остальные раскрыты полно), ИЛИ один-два аспекта раскрыты неполно. Продолжительность высказывания – 7–9 фраз; **2 балла –** коммуникативная задача выполнена не полностью: два аспекта не раскрыты (остальные раскрыты полно), ИЛИ все аспекты раскрыты неполно. Продолжительность высказывания – 4–6 фразы; **1 балл –** коммуникативная задача выполнена менее чем на 50%; три и более аспекта содержания не раскрыты. Продолжительность высказывания – 1–3 фразы. Критерий «Организация высказывания» **3 балла** – высказывание логично и имеет завершённый характер; имеются вступительная и заключительная фразы, соответствующие теме. Средства логической связи используются правильно; **2 балла –** высказывание в основном логично и имеет достаточно завершённый характер, НО отсутствует вступительная или заключительная фраза И/ИЛИ средства

			логической связи используются недостаточно; **1 балл –** высказывание нелогично И/ИЛИ не имеет завершенного характера, вступительная и заключительная фразы отсутствуют, средства логической связи практически не используются. **Критерий 3** «Языковое оформление высказывания» **3 балла** – используемый словарный запас, грамматические структуры, фонетическое оформление высказывания соответствуют поставленной задаче (допускается не более двух негрубых лексико-грамматических ошибок И/ИЛИ не более двух негрубых фонетических ошибок); **2 балла –** используемый словарный запас, грамматические структуры, фонетическое оформление высказывания в основном соответствуют поставленной задаче (допускается не более четырёх лексико-грамматических ошибок (из них не более двух грубых) И/ИЛИ не более четырёх фонетических ошибок (из них не более двух грубых); **1 балл –** понимание высказывания затруднено из-за многочисленных лексико-грамматических и фонетических ошибок (пять и более лексико-грамматических ошибок И/ИЛИ пять и более фонетических ошибок) ИЛИ более двух грубых ошибок. Удельный вес беседы составляет сумму баллов по всем трём критериям. Максимально 10 из 50 1**.Реферирование профессионально-ориентированного текста**. Реферирование оценивается по 3 основным критериям, каждый из которых может быть оценен по 4 балльной шкале (4-1). Критерий «Решение коммуникативной задачи» **4 балла** – основные положения текста/ точки зрения автора изложены; **3 балла** – основные положения текста/ точки зрения автора изложены, но часть из них представлена не в полном объёме; **2 балла** – основные положения текста/ точки зрения автора изложены избыточно ИЛИ недостаточно; **1 балл** – объём высказывания недостаточен, стиль не соответствует цели коммуникации Критерий «Организация высказывания» **3 баллов** – текст высказывания логично организован: присутствуют введение в проблему, ссылки на точку зрения автора, выводы по статье, используются надлежащие связующие элементы (не более одной ошибки);
Экзамен		В конце 4 семестра	**2 балла** – текст высказывания в целом логично организован: может отсутствовать введение или заключение; допускаются негрубые ошибки (2-3) в использовании связующих элементов; **1 балл** – идеи представлены хаотично, связующие элементы использованы не систематически или не использованы вообще; Критерий «Грамотность изложения» **3 баллов** – используемый словарный запас, грамматические структуры в основном соответствуют поставленной задаче, допускается не более 1-2 лексико-грамматических ошибки; **2 балла** – используемый словарный запас, грамматические структуры в основном соответствуют

			поставленной задаче (допускается не более четырёх лексико-грамматических ошибок); **1 балл** – используемый словарный запас, грамматические структуры большей частью не соответствует поставленной задаче; присутствуют многочисленные грубые ошибки (пять и более лексико-грамматических ошибок). Удельный вес реферирования составляет сумму баллов по всем трём критериям. Максимум – 10 баллов 2.**Беседа по пройденным темам** оценивается по 3 основным критериям, каждый из которых может быть оценен по 4 балльной шкале (1-4). <u>Критерий 1 «Решение коммуникативной задачи»</u> **4 балла** – коммуникативная задача выполнена полностью: содержание полно, точно и развёрнуто отражает все аспекты, указанные в задании. Продолжительность высказывания – 10-12 фраз; **3 балла** – коммуникативная задача выполнена частично: один аспект не раскрыт (остальные раскрыты полно), ИЛИ один-два аспекта раскрыты неполно. Продолжительность высказывания – 7–9 фраз; **2 балла –** коммуникативная задача выполнена не полностью: два аспекта не раскрыты (остальные раскрыты полно), ИЛИ все аспекты раскрыты неполно. Продолжительность высказывания – 4–6 фразы; **1 балл –** коммуникативная задача выполнена менее чем на 50%; три и более аспекта содержания не раскрыты. Продолжительность высказывания – 1–3 фразы. <u>Критерий «Организация высказывания»</u> **3 балла** – высказывание логично и имеет завершённый характер; имеются вступительная и заключительная фразы, соответствующие теме. Средства логической связи используются правильно; **2 балла –** высказывание в основном логично и имеет достаточно завершённый характер, НО отсутствует вступительная или заключительная фраза И/ИЛИ средства логической связи используются недостаточно; **1 балл –** высказывание нелогично И/ИЛИ не имеет завершенного характера, вступительная и заключительная фразы отсутствуют, средства логической связи практически не используются. **<u>Критерий 3</u>** <u>«Языковое оформление высказывания»</u> **3 балла** – используемый словарный запас, грамматические структуры, фонетическое оформление высказывания соответствуют поставленной задаче (допускается не более двух негрубых лексико-грамматических ошибок И/ИЛИ не более двух негрубых фонетических ошибок); **2 балла –** используемый словарный запас, грамматические структуры, фонетическое оформление высказывания в основном соответствуют поставленной задаче (допускается не более четырёх лексико-грамматических ошибок (из них не более двух грубых) И/ИЛИ не более четырёх фонетических ошибок (из них не более двух грубых); **1 балл –** понимание высказывания затруднено из-за многочисленных лексико-грамматических и фонетических ошибок (пять и более лексико-грамматических ошибок И/ИЛИ пять и более фонетических ошибок) ИЛИ более двух грубых ошибок. Удельный вес беседы составляет сумму баллов по всем трём критериям.

Литература

New English File : Intermediate student's book /Clive Oxenden, Christina Latham-Koenig Oxenden, Clive Oxford [a. o.] : Oxford University Press , [2009], 159 p.
2. Santiago Remacha Esteras Infotech. English for Computer Users// Cambridge University Press, 2008/
3.Verginia Evans, Jeney Dooley, Enroco Pontelli, Career Path Software Engeneering// Express Publishing, 2014

Дополнительные рекомендации к дисциплине

Для успешного изучения дисциплины «Иностранный язык», необходимо в обязательном порядке посещать практические занятия, вести поурочный словарь незнакомой лексики, тщательно конспектировать обсужда-емый языковой материал и правильно организовать самостоятельную работу. На практических занятиях студенты учатся оперировать изучаемой лексикой и грамматикой в разных ситуациях общения; со-вершенствуют языковые и речевые навыки – грамматически и лексически грамотно излагать проблемы в рамках заданной темы, свободно высказывать свои мысли и суждения, вести беседу, диалог/полилог, а также профессионально и качественно выполнять практические задания по темам и разделам дисциплины.

Б1.Б.1.04 Безопасность жизнедеятельности
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	Специалитет	4 курс 8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Беляев В.А., канд. тех. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
История; Экономика	Социальная инженерия

Цель и задачи дисциплины

Цель дисциплины – создание защиты человека в техносфере от внешних негативных воздействий антропогенного, техногенного и естественного происхождения, выработка идеологии безопасности, формирование безопасного мышления и поведения

Результаты обучения	Методы обучения	Методы оценивания
Объясняет основные принципы и правила безопасного поведения в повседневной жизни и в условиях чрезвычайных ситуаций. Предпринимает необходимые действия по обеспечению безопасности в повседневной жизни и в условиях чрезвычайных ситуаций. Обеспечивает безопасные и/или комфортные условия труда на рабочем месте.	• Лекции	• Тесты • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
1. Введение. Предмет БЖД	1					8	Изучение теоретического материала по теме 1.
2. Человек и среда обитания	1					8	Изучение теоретического материала по теме2.
3. Обеспечение комфортных условий жизнедеятельности	2					8	Изучение теоретического материала по теме 3.
4. Основы электробезопасности	2					8	Изучение теоретического материала4.
5. Воздействие электромагнитных излучений на человека и среду обитания	2					8	Изучение теоретического материала 5.
6. Безопасность и экологичность технических систем	3					8	Изучение теоретического материала 6.
7. Основы комплексной безопасности в повседневной жизни	3					9,05	Изучение теоретического материала7.
Консультации в семестре				0,95			
Прохождение промежуточной аттестации							
Всего:	14			0,95		57,05	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	**Зачтено**: студент владеет большей частью теоретического материала, но может иметь некоторые проблемы в знаниях, допускать негрубые ошибки; **Не зачтено**: студент не освоил большую часть теоретического материала.

Литература

Девисилов В.А., Белов С.В., Ильницкая А.В. Безопасность жизнедеятельности – М.: Высшая школа, 2009.

Белов, С.В. Безопасность жизнедеятельности и защита окружающей среды – М.: Юрайт, ИД Юрайт, 2013.

Дополнительные рекомендации к дисциплине

Занько Н.Г, Малаян К.Р. Русак О. Н. Безопасность жизнедеятельности – СПб.: Лань, 2008.

Б1.Б.1.05 Физическая культура и спорт
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	Специалитет	1 курс 1 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Иноземцева Татьяна Андреевна, старший преподаватель	Факультет физической культуры, кафедра физической культуры и спорта

Пререквизиты	Параллельно осваиваемые дисциплины
	Групповая динамика(Б1.У.В.ДВ.01.01)

Цель и задачи дисциплины

Цель дисциплины - формирование физической культуры личности студента и способности реализовать ее в социально-профессиональной, физкультурно-спортивной и оздоровительной деятельности.
Задачи дисциплины: всестороннее развитие и совершенствование личности, формирование отношений к здоровому образу жизни.

Результаты обучения	Методы обучения	Методы оценивания
Понимает роль физической культуры и спорта в современном обществе, в жизни человека, подготовке его к социальной и профессиональной деятельности, значение физкультурно-спортивной активности в структуре здорового образа жизни и особенности планирования оптимального двигательного режима с учетом условий будущей профессиональной деятельности. Использует методику самоконтроля для определения уровня здоровья и физической подготовленности в соответствии с нормативными требованиями и условиями будущей профессиональной деятельности. Составляет комплекс упражнений в соответствии с группой здоровья, комплексы профессионально-прикладной физической культуры с учетом особенностей будущей профессиональной деятельности.	• Лекции • Практики	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
1. Гимнастика.	2	4				8	Изучение теоретического материала по темам 1.
2. Прикладные упражнения.	2	4				8	Изучение теоретического

							материала по теме 2.
3. Плавание.	2	4				8	Изучение теоретического материала по теме 3.
4. Атлетическая гимнастика.	2	4				8	Изучение теоретического материала 4.
5. Волейбол.	2	4				8,25	Изучение теоретического материала 5.
Консультации в семестре				1,5			
Прохождение аттестации в форме зачета					0,25		
Всего:	10	20		1,5	0,25	40,25	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Тесты	80%	В течение семестра	**Зачтено**: более 40% правильных ответов; **Не зачтено**: менее 40% правильных ответов.
Зачет	20%	В конце семестра	**Зачтено**: студент полностью владеет теоретическим материалом; **Не зачтено**: не освоил большую часть теоретического материала.

Литература

1. Письменский И. А., Аллянов Ю. Н. Физическая культура: учебник для академического бакалавриата. Москва: Юрайт, 2016.
2. Барчуков И. С. Физическая культура: методики практического обучения. Москва: Кнорус, 2014.

Б1.Б.1.06 Основы информационной безопасности
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	6 курс 11 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Операционные системы, Компьютерные сети	Организационное и правовое обеспечение информационной безопасности

Цель и задачи дисциплины

Цель дисциплины – обучить студентов основам информационной безопасности, методам и алгоритмам защиты информации.
Задачи дисциплины: формирование базовых понятий информационной безопасности; формирование базовых знаний о законодательстве в области информационной безопасности

Результаты обучения	Методы обучения	Методы оценивания
Знает типовые проектные решения по обеспечению защищенности компьютерной системы; основные средства и способы обеспечения информационной безопасности; защитные механизмы и средства обеспечения безопасности к компьютерной системе. Умеет анализировать компьютерные системы с учетом требований к их защищенности, разрабатывать системы безопасности с учетом требований к их защищенности; экспериментально исследовать компьютерную систему и определять уровень защищенности этой системы.	• Лекции • Самостоятельная работа	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Понятие информационной безопасности. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности	4					10	Изучение учебного материала
Угрозы информационной безопасности	6					10	Изучение учебного материала
Обеспечение информационной безопасности объектов информационной сферы	6					10	Изучение учебного материала
Общая характеристика комплексной защиты информации (КЗИ)	5					10	Изучение учебного материала
Конфиденциальные документы	5					10	Изучение учебного материала
Организация и аудит КЗИ	6					10	Изучение учебного материала
Подготовка к прохождению				1,6		14,15	Подготовка к сдаче зачета

аттестации в форме зачета							
Прохождение аттестации в форме зачета					0,25		
Всего	32			1,6	0,25	74,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	**Зачтено**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает негрубые ошибки; **Незачтено**: студент не освоил большую часть теоретического материала.

Литература

1. Бабенко Л. К., Ищукова Е. А. Криптографическая защита информации: симметричное шифрование. – М.: Юрайт, 2019.
2. Васильева И. Н. Криптографические методы защиты информации. – М.: Юрайт, 2018.
3. Мельников Д. А. Информационная безопасность открытых систем. – М.: Флинта, 2013.
4. Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2014.
5. Платонов В. В. Программно-аппаратные средства защиты информации. – М.: Академия, 2014.
6. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах. – М.: Инфра-М, 2015.

Б1.Б.1.07 Языки программирования
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
10 з.е.	специалитет	2 курс 3 семестр 3 курс 5, 6 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Самохина Светлана Ивановна, к.ф.-м.н., доцент	Кафедра компьютерной безопасности ИПМКН

Пререквизиты	Параллельно осваиваемые дисциплины
Информатика, алгоритмы и структуры данных.	Научно-исследовательская работа, системы управления базами данных.

Цель и задачи дисциплины

Цель и задачи дисциплины – в 3 семестре – обучение объектно-ориентированному программированию, в 5 семестре изучение языка низкого уровня Ассемблер, в 6 семестре - обучение языкам программирования высокого уровня C# и Pyton.

Результаты обучения	Методы обучения	Методы оценивания
Способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения. Способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач. Способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	• Лекции • Лабораторные работы • Самостоятельная работа	• Прием лабораторных работ • Контрольные работы • Зачет • Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен/Зачет	Часы СРС	Задания
3 семестр							
Классы и объекты. Перегрузка операций в классе. Массивы объектов. Класс-шаблон. Агрегированные классы. Обработка исключительных ситуаций	14		28			10	Изучение учебного материала. Подготовка к лабораторным занятиям
Наследование. Полиморфизм. Раннее и позднее связывание. Виртуальные функции.	6		4			10	
Библиотека стандартных классов-	6					10	

шаблонов.							
Учебный класс Факультет.	6					10,8	
Подготовка к сдаче экзамена				3,2		33,7	
Сдача экзамена				2	0,3		
Итого	32		32	5,2	0,3	74,5	
5 семестр							
Регистровая структура универсального микропроцессора	4					2	Изучение теоретического материала.
Команды языка Ассемблер. Системные вызовы. Организация ввода и вывода данных	4		4			4	Изучение теоретического материала. Выполнение лабораторных работ.
Переходы	4		4			4	Изучение теоретического материала. Выполнение лабораторных работ
Команды управления циклом	2		4			4	Изучение теоретического материала. Выполнение лабораторных работ.
Работа с массивами	4		6			6	Изучение теоретического материала. Выполнение лабораторных работ.
Поразрядные операторы. Сдвиги. Организация деления и умножения с помощью операторов сдвига	4		4			4	Изучение теоретического материала. Выполнение лабораторных работ.
Процедуры. Работа со стеком	4		4			4	Изучение теоретического материала. Выполнение лабораторных работ.
Математический сопроцессор. Работа с вещественными числами и математическими функциями	6		6			6	Изучение теоретического материала. Выполнение лабораторных работ.
Индивидуальные консультации по дисциплине Подготовка к прохождению аттестации в форме зачета				3,45		6,55	Подготовка к сдаче зачета
Прохождение аттестации в форме зачета					0,3		
Итого	32		32	3,45	0,3	40,55	
6 семестр							
Основные понятия языка C#	4		4			4	Изучение теоретического материала. Выполнение лабораторных работ.
Символы и строки	2		2			2	Изучение теоретического материала. Выполнение лабораторных работ.
Основы объектно-ориентированного программирования в C#	4		4			4	Изучение теоретического материала. Выполнение лабораторных работ.
Обработка исключительных ситуаций	2		2			2	Изучение теоретического

							материала. Выполнение лабораторных работ.
Делегаты	2		2			2	Изучение теоретического материала. Выполнение лабораторных работ.
События и коллекции	2		2			2	Изучение теоретического материала. Выполнение лабораторных работ.
Контрольная работа			2			4	
Основы языка Pyton	4		4			4	Изучение теоретического материала. Выполнение лабораторных работ.
Обработка табличных данных и их визуализация	6		4			6	Изучение теоретического материала. Выполнение лабораторных работ.
Работа с векторами и матрицами	6		6			6	Изучение теоретического материала. Выполнение лабораторных работ.
Индивидуальные консультации по дисциплине Подготовка к прохождению аттестации в форме контрольной работы и зачета				3,45		4,55	Подготовка к сдаче зачета
Прохождение аттестации в форме зачета					0,3		
Итого	32		32	3,45		40,55	
Всего	96		96	12,1	0,3	155,6	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100%	В конце семестра	Выполненные лабораторные работы **Отлично**: студент полностью владеет теоретическим материалом; **Хорошо**: студент полностью владеет теоретическим материалом, но допускает ошибки или неточности; **Удовлетворительно**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает ошибки; **Неудовлетворительно**: студент не сдал все лабораторные работы и/или не освоил большую часть теоретического материала.
Зачет	100%		**Зачтено**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает негрубые ошибки; **Незачтено**: студент не освоил большую часть теоретического материала.

Литература

1. Таненбаум Э. С. Архитектура компьютера / Э. Таненбаум, Т. Остин ; [пер. с англ. Е. Матвеев]. - 6-е изд.. - Санкт-Петербург [и др.] : Питер, 2015. - 811 с.: рис., табл. - (Серия "Классика computer science").

2. Андреева В. В. Программирование на языке C# : учебное пособие : [для бакалавров направлений подготовки "Прикладная математика и информатика", "Математика и компьютерные науки" и др.] / В. В. Андреева, С. И. Самохина, А. Е. Петелин ; М-во науки и высш. образования, Нац. исслед. Том. гос. ун-т. - Томск : Издательский Дом Томского государственного университета, 2019. - 108 с.: ил., табл.. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000660298
3. Самоучитель Pyton https://pythonworld.ru/samouchitel-python

Б1.Б.1.08 Операционные системы
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
6 з.е.	специалитет	4 курс 7, 8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Языки программирования	Основы построения защищённых компьютерных сетей

Цель и задачи дисциплины

Цель: познакомить студентов с основными режимами работы процессоров на примере процессора семейства x86, механизмами организации и работы с памятью, а также основными способами взаимодействия процессов в системе. Рассмотреть механизм исключений на примере процессоров семейства x86, общее устройство файловых систем, способы реализации многозадачности в ОС.

Задачи:

- Дать представление о теоретических основах работы процессора.
- Разработать прототип ОС, а именно, загрузчик операционной системы, переход в защищенный режим, а также реализовать вывод на экран в защищенном режиме.
- Реализовать обработчик исключений, реализовать многозадачность и ввод с клавиатуры.

Результаты обучения	Методы обучения	Методы оценивания
ОПК-7. Обучающийся будет: знать основные механизм работы ОС; устройство основных механизмов работы ОС на примере конкретных ОС (Unix); алгоритмы управления памятью, планирования процессов и потоков; уметь реализовывать базовую функциональность ОС; решать практические задачи с применением алгоритмов управления памятью, планирования процессов, задачи межпроцессорного взаимодействия; владеть навыками работы в ОС Linux, с программными эмуляторами работы процессоров bochs и Qemu, написания и отладки низкоуровневого кода на языке С и ассемблер. ПК-17. Обучающийся будет знать процесс загрузки ОС Linux; устройство основных механизмов работы с аппаратурой (udev, hal), с дисками, методов виртуализации, механизмов создания пользовательских файловых систем; механизхмы управления памятью и другими ресурсами процесса или группы процессов в ОС Linux; устройство файловой системы ОС Linux. Уметь настраивать основные механизмы работы ОС и исправлять неполадки в их работе; настраивать ограничения на работу процессов в системе, управлять ресурсами в системе. Владеть навыками настройки основных механизмов ОС и отладки их работы.	• Лекции • Лабораторные занятия • Самостоятельная работа	• Контрольные работы • Экзамен • Зачет

Содержание дисциплины		
Темы занятий	**Контактные часы**	**Самостоятельная работа**

	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
7 семестр							
Введение в предмет. Эволюция ОС. Классификация ОС	10	5		0,6		4	Изучение учебного материала; выполнение контрольных заданий
Режимы работы процессора. Реальный режим работы процессора. BIOS и UEFI. Загрузчики ОС Linux	11	5		0,6		4	Изучение учебного материала; выполнение контрольных заданий
Режимы работы процессора. Защищенный режим работы.	11	6		1		4	Изучение учебного материала; выполнение контрольных заданий
Виртуальная память. Принцип работы, реализация в процессорах x86. Многозадачность и ее виды.	11	5		0,8		4	Изучение учебного материала; выполнение контрольных заданий
Многозадачность и ее виды. Алгоритмы планирования работы процессора при различных видах многозадачности	11	6		1		4	Изучение учебного материала; выполнение контрольных заданий
Межпроцессорное взаимодействие.	10	5		0,8		5,2	Изучение учебного материала; выполнение контрольных заданий
Промежуточная аттестация в форме экзамена				2	0,3	15,7	Подготовка к сдаче экзамена
Итого	64	32		6,8	0,3	40,9	
8 семестр							
Примитивы синхронизации процессов		8				8	Изучение учебного материала; выполнение контрольных заданий
Управление памятью		8				8	Изучение учебного материала; выполнение контрольных заданий
Механизм прерываний процессора		8				8	Изучение учебного материала; выполнение контрольных заданий
Файловые системы		8				8	Изучение учебного материала; выполнение контрольных заданий
Промежуточная аттестация в форме зачета				1,6	0,25	6,15	Подготовка к зачету
Итого		32		1,6	0,25	38,15	
ИТОГО	64	64		8,4	0,55	79,05	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен Зачет	100%	В сессию	Оценка «Отлично» - обучающийся хорошо знает принципы устройства механизмов ОС и возможное их применение. Оценка «Хорошо» - обучающийся знает основные принципы устройства механизмов ОС

			Оценка «Удовлетворительно»/зачтено - обучающийся знает основные понятия курса: сегментная и страничная организация памяти, безопасный и реальный режим работы процессора, механизм исключений процессора, примитивы синхронизации и межпроцессного взаимодействия, файловые системы. Оценка «Неудовлетворительно»/Незачтено - обучающийся не знает основные понятия курса.

Литература
1. Столлингс В. Операционные системы. М.: Издательский дом «Вильямс», 2014. – 848 с. 2. Таненбаум Э. Современные операционные системы. СПб.: Питер, 2016. – 576 с.
Дополнительные рекомендации к дисциплине
http://osdev.org

Б1.Б.1.09 Системы управления базами данных
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	3 курс 5 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Мокина Елена Евгеньевна, старший преподаватель	кафедра теоретических основ информатики

Пререквизиты	Параллельно осваиваемые дисциплины
Информатика	

Цель и задачи дисциплины

Цель: формирование представлений о структуре и функциях реляционных систем управления базами данных (СУБД)

Задачи:

– рассмотреть класс реляционных СУБД;

– изучить математические основы реляционных СУБД (рассмотреть начальную алгебру Кодда, теорию нормализации);

– изучить язык манипулирования данными в реляционных СУБД – SQL

Результаты обучения	Методы обучения	Методы оценивания
Знать: программные средства общего и специального назначения, включая СУБД; принципы построения СУБД и особенности их применения; физическую организацию баз данных и принципы (основы) их защиты. **Уметь**: работать с программными средствами общего и специального назначения, включая СУБД; производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая системы управления базами данных **Владеть**: навыками работы с программными средствами общего и специального назначения в области защиты информации, включая СУБД	• Лекции • Лабораторные работы • Самостоятельная работа	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Общие сведения о базах данных. Модели данных.	4					10	Изучение учебного материала.
Математическая модель. Семантическая модель. Логическая модель данных. Физическая модель данных.	4					10	Изучение учебного материала.

Проектирование баз данных (ER-модель. Построение диаграммы при моделировании предметной области. Схема реляционной базы данных. Правила порождения схемы из диаграммы, пример)	8		4			10	Изучение учебного материала. Подготовка к лабораторным занятиям
Язык запросов SQL (Общая характеристика языка SQL. Различные конструкции запросов выборки данных)	8		8			10	Изучение учебного материала. Подготовка к лабораторным занятиям
Нормализация реляционных баз данных (Функциональные зависимости в отношениях. Неполные зависимости. 2НФ. Транзитивная зависимость. 3НФ. Нормальная форма Бойса-Кодда (БКНФ))	8		4			10	Изучение учебного материала. Подготовка к лабораторным занятиям
Подготовка к сдаче зачета				2,4		7,35	
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего	32		16	2,4	0,25	57,35	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Лабораторные работы	50 %	В течение семестра	Должно быть сдано более 65% лабораторных работ;
Зачет	100 %	В конце семестра	Должны быть сданы обязательные лабораторные работы, иначе оценка "Неудовлетворительно". **Отлично**: студент полностью владеет теоретическим материалом; **Хорошо**: студент полностью владеет теоретическим материалом, но допускает ошибки или неточности; **Удовлетворительно**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает ошибки; **Неудовлетворительно**: студент не сдал обязательные лабораторные работы и/или не освоил большую часть теоретического материала.

Литература

Основная литература

1. Дэйт К. Дж. Introduction to Database Systems: Введение в системы баз данных/К.Дж.Дэйт -М.: Вильяме, 2016. - 1328 с.
2. Кузнецов С.Д. Базы данных/С.Д. Кузнецов - М.: Academia, 2012 - 496 с.
3. Грофф Дж. Р. SQL. Полное руководство/ Дж.Р. Грофф, П.Н. Вайнберг, Э.Дж. Оппель -М.: Вильяме, 2014. - 960 с.

Дополнительная литература

1. Кузнецов С.Д. Базы данных. Модели и языки/С .Д. Кузнецов - М.: Бином-Пресс, 2008. -720с.
2. Date C. J. Database in Depth: Relational Theory for Practitioners/C. J. Date - Sebastopol, CA: CTReilly Media, 2005. - 230 с.
3. Тахагхогхи С. Руководство по MySQL/С. Тахагхогхи, Х.Е. Вильяме - М.: Русская редакция, 2007. - 544 с.
4. Грабер М. SQL. Справочное руководство/ М. Грабер - М.: Лори, 2006. - 368 с.

Дополнительные рекомендации к дисциплине

1. Упражнения по SQL [Электронный ресурс] http://www.sql-ex.ru/

Б1.Б.1.10 Электроника и схемотехника
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	4 курс8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Беляев В.А., канд. тех. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Физика; Дискретная математика; теория автоматов; теория булевых функций	Аппаратная реализация криптоалгоритмов, Физика

Цель и задачи дисциплины

Цель – ознакомление обучающихся с основными этапами и технологиями проектирования и создания больших интегральных схем.

Задачи: обеспечить приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействовать формированию научного мировоззрения и системного мышления при разработке сложных цифровых устройств.

Результаты обучения	Методы обучения	Методы оценивания
Овладение знаниями и основными понятиями в области принципов работы цифровой электроники, математическими моделями и базовыми элементами цифровых схем, схемами включения этих элементов, алгоритмами проектирования цифровых устройств.	• Лекции • Контрольные работы • Лабораторные работы	• Тесты • Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Модели цифровых устройств	2		2			2	Изучение учебного материала. Подготовка к занятиям
Переключательные элементы	2		2			2	Изучение учебного материала. Подготовка к занятиям
Построение базовых логических схем на переключательных элементах	2		2			2	Изучение учебного материала. Подготовка к занятиям
Цифровая абстракция. Логические уровни	2		2			1	Изучение учебного материала. Подготовка к занятиям
Передаточная характеристика логических вентилей	2		2			1	Изучение учебного материала. Подготовка к занятиям
Базовые комбинационные блоки. Временные характеристики	2		2			2	Изучение учебного материала. Подготовка к занятиям
Мультиплексоры	2		2			2	Изучение учебного материала. Подготовка к занятиям
Дешифраторы	2		2			1	Изучение учебного материала. Подготовка к занятиям

Проектирование последовательностной логики	2		2			1	Изучение учебного материала. Подготовка к занятиям
Полупроводники n- и p-типа. P-n переходы, n-МОПи p-МОП транзисторы.	2		2			1	Изучение учебного материала. Подготовка к занятиям
КМОП транзисторы	2		2			1	Изучение учебного материала. Подготовка к занятиям
Технология производства БИС и СБИС.	2		2			1	Изучение учебного материала. Подготовка к занятиям
Области и уровни моделей в проектировании СБИС.	2		2			1	
Уровни и процесс проектирования СБИС.	2		2			1	Изучение учебного материала. Подготовка к занятиям
Диаграмма Гайского-Кана (Gajski and Kuhn)	2		2			1	Изучение учебного материала. Подготовка к занятиям
Блочно-ориентированное проектирование СБИС (Block-based design)	2		2			2,8	Изучение учебного материала. Подготовка к занятиям
Подготовка к прохождению экзамена				3,2		15,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего:	32		32	5,2	0,3	38,5	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100%	В конце семестра	**Отлично/хорошо/удовлетворительно**: степень владения теоретическим материалом **Неудовлетворительно**: студент не освоил большую часть теоретического материала.

Литература

1. Угрюмов Е. П. Цифровая схемотехника: Учеб. пособие для вузов. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2007. — 800 с.: ил..
2. Дэвид М. Харрис и Сара Л. Харрис. Цифровая схемотехника и архитектура компьютера. второе издание. Издательство Morgan Kaufman, English Edition 2013.

Дополнительные рекомендации к дисциплине

1. Кучумов А.И. Электроника и схемотехника. – М.: Гелиос АРВ, 2005, гриф УМО в области информационной безопасности.

Б1.Б.1.11 Организационное и правовое обеспечение информационной безопасности
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалите	6 курс 11 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Генрих Виктор Витальевич	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Социальная инженерия	Основы информационной безопасности

Цель и задачи дисциплины

Цель: ознакомить студентов с основными законодательными и подзаконными актами в области защиты информации; научить использовать нормативные правовые акты и методические документы в области информационной безопасности, в т.ч. регулирующие вопросы организации лицензирования и оценки соответствия в Российской Федерации; обучить анализу и оценке угроз информационной безопасности, в частности, связанных с утечкой информации по техническим каналам утечки информации, а также выявляемых при разработке системы защиты информации в информационных системах персональных данных; обучить общим принципам организации защиты информации с применением модели угроз и модели нарушителя.

Задачи:

- сформировать знания нормативных правовых актов в области защиты информации;
- сформировать умения и навыки анализа основных правовых актов, определения правовой оценки информации, используемой в профессиональной деятельности;
- сформировать профессиональный минимум, необходимый для подбора и изучения текстов, нормативных документов в сфере информационной безопасности;
- сформировать способность организовывать работы по выполнению режима защиты информации, в т.ч. ограниченного доступа;
- сформировать способность применения нормативных правовых актов и нормативных методических документов в области обеспечения информационной безопасности, а также способность разработки проектов нормативных документов и методических материалов, регламентирующих обеспечение информационной безопасности в организации.

Результаты обучения	Методы обучения	Методы оценивания
Обучающийся сможет: - использовать нормативные правовые акты в области защиты информации (в т.ч. при реализации/модернизации системы защиты информации объекта информатизации). - анализировать основные правовые акты, давать правовую оценку информации, используемой в профессиональной деятельности. - подбирать и изучать научно-техническую литературу, изучать и отбирать правовые и нормативные акты в области обеспечения информационной безопасности. - использовать применяемые в сфере защиты информации нормативные правовые акты и методические документы по организации: лицензирования; сертификации средств защиты информации; аккредитации; аттестации объектов информатизации. - анализировать и оценивать угрозы информационной безопасности объекта защиты информации. - применять нормативные правовые акты и нормативные методические документы в области защиты информации (в т.ч. определяющие вопросы внедрения/применения средств и мер по защите информации), а также разрабатывать проекты нормативных документов, регламентирующих обеспечение информационной безопасности в организации.	• Лекции	• Проверка конспектов самоподго-товки • Вопросы • Опросы на занятиях • Домашние задания • Коллоквиум • Зачет

Содержание дисциплины							
Темы занятий	**Контактные часы**					**Самостоятельная работа**	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
1. Введение: правовые основы, информация как объект права; правовое регулирование в области защиты информации; органы исполнительной власти, осуществляющие регулирование; закон об информации, информационных технологиях и защите информации; регулирование использования международной сети Интернет.	7			0,2		4	Разбор лекционного материала по конспектам лекций, учебным пособиям, научно-технической литературе и нормативным правовым актам, касающегося правового регулирования в области обеспечения информационной безопасности.
2. Лицензирование и оценка соответствия: лицензирование в области защиты информации; формы оценки соответствия, сертификация средств защиты информации по требованиям безопасности; аккредитация; аттестация объектов информатизации, нормативные документы ФСБ и ФСТЭК по аттестации.	10			0,5		19	Разбор лекционного материала по конспектам лекций, нормативным правовым актам, касающегося лицензирования и оценки соответствия. Выполнение домашних заданий с целью научиться выбирать сертифицированные средства защиты информации, удовлетворяющие заданным требованиям (в соответствии с нормативными документами ФСБ и ФСТЭК России).
3. Технические каналы утечки информации.	3			0,4		8	Разбор лекционного материала по конспектам лекций, учебным пособиям, научно-технической литературе и нормативным правовым актам, касающегося принципов реализации технических каналов утечки информации и способов их нейтрализации. Выполнение домашних заданий с целью научиться определять технические каналы утечки информации для заданного объекта информатизации и способы их нейтрализации.
4. Законодательство в области защиты персональных данных: общие сведения по законодательству в области персональных данных; закон о персональных данных, уровни защищенности информационных систем персональных данных; требования ФСБ по защите информационных систем персональных данных; требования ФСТЭК по защите информационных систем персональных данных; модели угроз, оценка актуальности угроз.	12			0,5		23	Разбор лекционного материала по конспектам лекций, нормативным правовым актам, учебным пособиям и научно-технической литературе, касающегося законодательства в области защиты персональных данных. Выполнение домашних заданий с целью научиться проводить мероприятия по обеспечению информационной безопасности информационных систем персональных данных.
Прохождение промежуточной аттестации в форме зачета					0,25	20,15	Подготовка к сдаче зачета. Сдача зачета.
Всего	32			1,6	0,25	74,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Вид оцениваемой работы: - Конспекты самоподготовки - Вопросы - Опросы на занятиях - Домашние задания - Коллоквиум - Зачет	 10 10 20 30 10 20	 В течение семестра В течение семестра В течение семестра В течение семестра В течение семестра В конце семестра	**Зачтено:** ≥ 60% от максимальной суммы баллов (полученных по результатам проверки конспектов самоподготовки, проведенных на занятиях устных/письменных опросов, коллоквиума, выполненных домашних заданий, а также по результатам зачета). Должны быть сданы домашние задания и коллоквиум. **Не зачтено:** <60% от максимальной суммы баллов (полученных по результатам проверки конспектов самоподготовки, проведенных на занятиях устных/письменных опросов, коллоквиума, выполненных домашних заданий, а также по результатам зачета). Не сданы домашние задания и коллоквиум.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102108264
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102108261
3. Указ президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017
4. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» от 27.12.2006 г. [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017
5. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» от 18.12.2008 г. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200075565
6. Бирюков А.А. Информационная безопасность: защита и нападение / А.А. Бирюков – М.: ДМК Пресс, 2016 – 474 с.
7. Аверченков В.И. Защита персональных данных в организации: монография / Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р. – М.: ФЛИНТА, 2016 – 124 с.
8. Каторин Ю.Ф. Защита информации техническими средствами / Каторин Ю.Ф., Разумовский А.В., Спивак А.И. – СПб: НИУ ИТМО, 2012 – 416 с.
9. Чубукова С.Г. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум. / Чубукова С.Г. – М.: Юрайт, 2016 – 326 с.
10. Постановление Правительства Российской Федерации от 03.02.2012 № 79 79 «О лицензировании деятельности по технической защите конфиденциальной информации» [Электронный ресурс]. URL: https://base.garant.ru/70136258/
11. Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» [Электронный ресурс]. URL: https://docs.cntd.ru/document/902342782
12. Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации» [Электронный ресурс]. URL: https://base.garant.ru/102670/
13. Приказ ФСТЭК России от 10.04.2015 № 33 «Об утверждении Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности» [Электронный ресурс]. URL: https://base.garant.ru/71038824/
14. Приказ Минцифры России от 29 октября 2020 года № 559 «Об утверждении Административного регламента

предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации удостоверяющих центров и Административного регламента осуществления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственного контроля (надзора) за соблюдением аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом "Об электронной подписи" и на соответствие которым эти удостоверяющие центры были аккредитованы» [Электронный ресурс]. URL: https://docs.cntd.ru/document/566210634
15. Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено Гостехкомиссией РФ 25.11.1994) [Электронный ресурс]. URL: https://docs.cntd.ru/document/902243370
16. Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» [Электронный ресурс]. URL: https://docs.cntd.ru/document/607749878
17. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс]. URL: https://base.garant.ru/70252506/
18. Приказ ФСТЭК России от 18 февраля 2013 года № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" [Электронный ресурс]. URL: https://docs.cntd.ru/document/499005278
19. Приказ ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [Электронный ресурс]. URL: https://base.garant.ru/70727118/
20. Мельников В.П. Защита информации / В.П. Мельников, А.И. Куприянов, А.Г. Схиртладзе – М. «Академия», 2014 – 304 с.
21. Ковалева Н.Н. Информационное право в России. Учебное пособие / Н.Н. Ковалева – М.: Дашков и КО, 2007 – 360 с.
22. Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере. Монография / А.К. Жарова – М.: Янус-К, 2016 – 248 с.
23. Бузов Г.А. Защита от утечки по техническим каналам: Учебное пособие / Бузов Г.А., Калинин С.В., Кондратьев А.В. – М.: Горячая линия-Телеком, 2005 – 416 с.
24. ГОСТ Р 53112-2008 «Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний» от 18.12.2008 г. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200075567

Дополнительные рекомендации к дисциплине

Для изучения нормативно-правовой документации в сфере информационной безопасности и самостоятельной работы рекомендуется использовать следующие информационно-справочные системы и электронные ресурсы:

1. http://www.kremlin.ru/acts/bank
2. http://pravo.gov.ru
3. http://www.consultant.ru
4. https://docs.cntd.ru
5. https://base.garant.ru

Б1.Б.1.12 Техническая защита информации
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	5 курс9 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Беляев В.А., канд. тех. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Физика; Дискретная математика; теория автоматов; теория булевых функций	Аппаратная реализация криптоалгоритмов, Физика, Криптографические методы защиты информации

Цель и задачи дисциплины

Цель – формирование у студентов научного мировоззрения, формирование профессиональных компетенций по специальности «Компьютерная безопасность» путём привития им знаний основ инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий, развитие в процессе обучения системного мышления.

Задачи: обеспечить приобретение знаний и умений необходимых для решения задач инженерно-технической защиты информации с учётом системного подхода.

Результаты обучения	Методы обучения	Методы оценивания
Овладение основными понятиями в области физических явлений и процессов при решении профессиональных задач, основами защиты от возможных информационных атак, способностью к общей оценке состояния информационной безопасности.	• Лекции • Лабораторные работы	• Тесты • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Системный подход к защите информации	2					4	Изучение учебного материала
Основные концептуальные положения ТЗИ	2					4	Изучение учебного материала
Информация как предмет защиты	2					4	Изучение учебного материала
Источники опасных сигналов	4		2			4	Изучение учебного материала Подготовка к лабораторной работе
Характеристика технической разведки	4		2			4	Изучение учебного материала Подготовка к лабораторной работе
Технические каналы утечки информации	2		2			4	Изучение учебного материала Подготовка к лабораторной работе
Распространение сигналов в технических каналах утечки информации	2		2			4	Изучение учебного материала Подготовка к лабораторной работе

Подавление опасных сигналов	2					4	Изучение учебного материала Подготовка к лабораторной работе
Средства технической разведки	2		2			4	Изучение учебного материала Подготовка к лабораторной работе
Средства инженерной защиты и технической охраны объектов	2		2			4	Изучение учебного материала Подготовка к лабораторной работе
Средства предотвращения утечки информации по техническим каналам	4		2			4	Изучение учебного материала Подготовка к лабораторной работе
Принципы оценки эффективности средств ТЗИ	4		2			4	Изучение учебного материала Подготовка к лабораторной работе
Прохождение промежуточной аттестации в форме зачета					0,25	9,35	
Всего:	32		16	2,4	0,25	57,35	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	**Зачтено**: студент владеет большей частью теоретического материала, но может иметь некоторые проблемы в знаниях, допускать негрубые ошибки; **Не зачтено**: студент не освоил большую часть теоретического материала.

Литература

1. Зайцев А.П. Технические средства и методы защиты информации. – М: Горячая линия-Телеком, 2012. – 615 с.
2. Ищейнов В.Я. Защита конфиденциальной информации. -М: Форум, 2013. – 256 с.
3. Царегородцев А.В. Технические средства защиты информации. Учебник. – М.: Изд. ВГНА Минфина России, 2009.
4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М: ФОРУМ, 2013. – 592 с.

Дополнительные рекомендации к дисциплине

2. Торокин А.А. Основы инженерно-технической защиты информации. - М.: «Ось-89», 1998.
3. Хорев А.А. Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации. - М.: Гостехкомиссия России, 1998.

Б1.Б.1.13 Модели безопасности компьютерных систем
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	5 курс 9 семестр	Обязательная, входит в базовую часть	Очное обучение	Русский

Преподаватель	Структурное подразделение
Твардовский Александр Сергеевич, к.ф.-м.н., старший преподаватель	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Дискретная математика, Информатика, Операционные системы, Дискретная математика. Теория автоматов, Алгебра, Компьютерные сети	Защита в операционных системах, Основы информационной безопасности

Цель и задачи дисциплины

Цель: изучить основные моделей безопасности компьютерных систем, модели дискреционного, мандатного, ролевого управления доступом, безопасности информационных потоков и изолированной программной среды.
Задачи:

- Изучить основные модели дискреционного, мандатного и ролевого управления доступом.
- Изучить модели безопасности информационных потоков и изолированной программной среды.
- Овладеть математическим аппаратом для разработки и анализа безопасности моделей управления доступом
- Рассмотреть вопросы разработки и реализации механизмов управления доступом.

Результаты обучения	Методы обучения	Методы оценивания
Знать: основные виды политик управления доступом и информационными потоками в компьютерных системах. **Уметь:** разрабатывать модели безопасности современных и перспективных компьютерных систем. **Владеть:** классическими моделями управления доступом. **Знать:** основные формальные модели дискреционного, мандатного, ролевого управления доступом. **Знать:** назначение и формальное описание классических моделей безопасности (ХРУ, TG, БЛП, ГД, ТМД). **Уметь:** разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем. **Знать:** модели изолированной программной среды и безопасности информационных потоков. **Владеть:** математическим аппаратом для разработки и анализа безопасности моделей управления доступом.	• Лекции • Изучение учебного материала • Решение задач на практических занятиях • Выполнение проектного задания	• Зачёт с оценкой • Устные опросы • Защита проекта

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачёт	Часы СРС	Задания
Основные элементы и виды управления доступом	6	2				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение проекта
Модель RBAC	2	4				2	Изучение учебного материала,

							подготовка к практическим занятиям, выполнение проекта
Take-Grant модель	4	6				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение проекта
Расширенная Take-Grant модель	4	6				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение проекта
Основные элементы ДП-моделей	4	2				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение проекта
Модель изолированной программной среды	4	2				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение проекта
Модели Белла-ЛаПадулы и Биба	4	4				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение проекта
Разработка механизмов управления доступом для современных компьютерным систем	4	6				5,8	Изучение учебного материала, подготовка к практическим занятиям, выполнение проекта
Индивидуальная консультация				3,2			
Групповая консультация				2			
Подготовка к прохождению промежуточной аттестации в форме зачёт с оценкой						6,75	
Прохождение промежуточной аттестации в форме зачёт с оценкой					0,25		
Всего	32	32		5,2	0,25	38,55	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Устные опросы	20%	В течение семестра	Корректные ответы на вопросы не менее чем по 50% тем
Проект	20%	В течение семестра	Проект выполнен и соответствует всем пунктам технического задания
Зачёт с оценкой	60%	В конце семестра	Отлично – знает основные виды политик управления доступом и информационными потоками в компьютерных системах, умеет разрабатывать модели безопасности современных и перспективных компьютерных систем, владеет классическими моделями управления доступом, знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, знает назначение и формальное описание классических моделей безопасности (ХРУ, TG, БЛП, ГД, ТМД), умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем, знает модели изолированной программной среды и безопасности информационных потоков, владеет математическим аппаратом для разработки и анализа безопасности моделей управления доступом. Хорошо – знает основные виды политик управления доступом и информационными потоками в

			компьютерных системах, владеет классическими моделями управления доступом, знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, знает основы разработки моделей угроз и модели нарушителя безопасности компьютерных систем, имеет представление об основах моделей изолированной программной среды и безопасности информационных потоков, хорошо владеет математическим аппаратом для разработки и анализа безопасности моделей управления доступом. Удовлетворительно – знает основные виды политик управления доступом и информационными потоками в компьютерных системах, обладает посредственными познаниями о формальных моделях дискреционного, мандатного, ролевого управления доступом, знает основы моделей угроз и модели нарушителя безопасности компьютерных систем, обладает посредственными познаниями об основах моделей изолированной программной среды и безопасности информационных потоков, бегло знаком с математическим аппаратом для разработки и анализа безопасности моделей управления доступом. Неудовлетворительно – не знает основные виды политик управления доступом и информационными потоками в компьютерных системах, не знает формальные модели дискреционного, мандатного, ролевого управления доступом, не знает основы моделей угроз и модели нарушителя безопасности компьютерных систем, не знаком с моделями изолированной программной среды и безопасности информационных потоков, не ориентируется в математическом аппарате для разработки и анализа безопасности моделей управления доступом.

Литература

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие для вузов / П.Н. Девянин. - Москва : Гор. линия-Телеком, 2012. – 320 с.
2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009. – 352 с.
3. Bishop, M. Computer security: Art and science, 2002. – 1084 p.
4. Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие. Екатеринбург: изд-во Урал. Ун-та, 2008. – 212 с.

Дополнительные рекомендации к дисциплине

1. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. – 176 с.
2. Владимир Кочетков. Философия Application Security. – URL: https://www.youtube.com/watch?v=mb7tcT-9VXk
3. Maarten Decat. Access Control. – URL: https://www.youtube.com/watch?v=7e0fMbnovMc
4. George Danezis. Access Control. – URL: https://www.youtube.com/watch?v=QaS_UBuPVWA
5. Колегов Д.Н. Моделирование безопасности управления доступом и информационными потоками на основе ДП-моделей. – URL: https://vimeo.com/97906604

Б1.Б.1.14 Криптографические методы защиты информации
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
8 з.е.	специалитет	4 курс 7,8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Языки программирования, Информатика Теория вероятностей и математическая статистика, Дискретная математика Математическая логика и теория алгоритмов Дискретная математика. Теория автоматов Теория чисел, Алгебра, Геометрия Профессиональный перевод специальной литературы, Введение в специальность 1,2 Введение в математику	Основы построения защищённых компьютерных сетей, Теория информации Основы построения защищённых баз данных Теоретико-числовые методы в криптографии Булевы функции в криптографии Теория вычислительной сложности

Цель и задачи дисциплины

Цель: формирование общих представлений о содержании криптографических методов защиты информации и о подходах к оценке эффективности таких методов.

Задачи:

- дать представление о базовых понятиях и задачах криптографии;
- ознакомить с современными стандартами криптографической защиты;
- дать представление о методах криптографического анализа.

Результаты обучения	Методы обучения	Методы оценивания
В результате изучения дисциплины студент должен **знать:** - основные задачи, решаемые криптографическими методами; - математические модели шифров, подходы к оценке их стойкости; - национальные и мировые стандарты в области криптографической защиты информации; **уметь:** - корректно использовать криптографические алгоритмы при решении задач защиты информации; - применять математические методы при исследовании криптографических алгоритмов.	• Лекции • Практика	• Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
7 семестр							
Основные понятия и задачи криптографии	4	4				6	Изучение учебного материала. Подготовка к практическим занятиям

Шифры замены и перестановки	8	8				13	Изучение учебного материала. Подготовка к практическим занятиям
Современные криптосистемы	20	20				21,8	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к экзамену				3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	32		5,2	0,3	74,5	
8 семестр							
Методы криптоанализа	22	22				24	Изучение учебного материала. Подготовка к практическим занятиям
Теория секретных систем Шеннона	4	4				6	Изучение учебного материала. Подготовка к практическим занятиям
Автоматная криптография	6	6				10,8	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к экзамену				3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	32		5,2	0,3	74,5	
Итого	64	64		10,4	0,6	149	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100%	В конце семестра	Отлично – студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на практических занятиях. Хорошо – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на практических занятиях. Удовлетворительно – студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на практических занятиях. Неудовлетворительно – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении заданий на практических занятиях.

Литература

1. Лось А.Б. Криптографические методы защиты информации: учебник для академического бакалавриата: Учебник / Лось А. Б., Нестеренко А. Ю., Рожков М. И. – М: Издательство Юрайт, 2018, – 473 с.
2. Бабаш А.В. Криптографические методы защиты информации: Учебно-методическое пособие: Том 1 /Национальный исследовательский университет "ВШЭ". Москва: Издательский Центр РИОР , 2019. – 413 с.
3. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата. - М.: Издательство Юрайт, 2017. - 209 с.
4. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата. - М.: Издательство Юрайт, 2017. - 245 с.

Дополнительные рекомендации к дисциплине
1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. М.: Гелиос АРВ, 2002, 480 с. 2. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. М.: Гелиос АРВ, 2006, 376 с. 3. Агибалов Г.П. Конечные автоматы в криптографии // Прикладная дискретная математика, 2009, Приложение № 2, С. 43–73 4. Кузьминов Т.В. Криптографические методы защиты информации / Т.В. Кузьминов. Новосибирск: Наука, 1998, 194 с. 5. Токарева Н.Н. Симметричная криптография. Краткий курс: учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2012, 234 с. 6. Курс "Основы криптографии" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/691/547/info (дата обращения: 01.03.2022) 7. Курс "Математика криптографии и теория шифрования» [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/552/408/info (дата обращения: 01.03.2022) 8. Курс "Криптографические основы безопасности" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/28/28/info (дата обращения: 01.03.2022)

Б1.Б.1.15 Криптографические протоколы
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
8 з.е.	специалитет	5 курс 9 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Языки программирования, Компьютерные сети Теория вероятностей и математическая статистика, Дискретная математика Математическая логика и теория алгоритмов Дискретная математика. Теория автоматов Теория чисел, Алгебра, Профессиональный перевод специальной литературы, Введение в специальность 1,2, Основы построения защищённых компьютерных сетей	Защита в операционных системах Сети и системы передачи информации Аппаратная реализация криптоалгоритмов Квантовые вычисления Постквантовая криптография Методы верификации Безопасность веб-приложений Анализ уязвимостей программного обеспечения

Цель и задачи дисциплины

Цель: формирование профессиональных компетенций в области анализа и синтеза криптографических протоколов, ознакомление с государственными и международными стандартами в этой области.

Задачи:

- дать представление о типовых криптографических протоколах;
- ознакомить с современными стандартами в этой области;
- дать представление об основных уязвимостях криптографических протоколов.

Результаты обучения	Методы обучения	Методы оценивания
В результате изучения дисциплины студент должен **знать:** - типовые криптографические протоколы и требования к ним - основные атаки на криптографические протоколы **уметь:** - проводить анализ безопасности криптографических протоколов **владеть:** - криптографической терминологией - инструментами анализа безопасности криптографических протоколов - навыками реализации прикладных криптографических протоколов	• Лекции • Лабораторные занятия	• Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
9 семестр							

Классификация криптографических протоколов	4		4			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Типовые криптографические протоколы и атаки на них	20		20			21,8	Изучение учебного материала. Подготовка к лабораторным занятиям
Прикладные криптографические протоколы (часть 1)	8		8			13	Изучение учебного материала. Подготовка к лабораторным занятиям
Подготовка к экзамену				3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32		32	5,2	0,3	74,5	
А семестр							
Прикладные криптографические протоколы (часть 2)	20					44,4	Изучение учебного материала.
Инструменты анализа безопасности криптографических протоколов	12					30	Изучение учебного материала.
Подготовка к экзамену				1,6		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32			3,6	0,3	108,1	
Итого	64		32	8,8	0,6	182,6	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100%	В конце семестра	Отлично – студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях. Хорошо – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях. Удовлетворительно – студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях. Неудовлетворительно – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Литература

1. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации: учебник для академического бакалавриата. - М.: Издательство Юрайт, 2016. - 473 с.
2. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата. - М.: Издательство Юрайт, 2017. - 209 с.
3. Фомичёв В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные

и прикладные аспекты: учебник для академического бакалавриата. - М.: Издательство Юрайт, 2017. - 245 с.
4. Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата. - М.: Издательство Юрайт, 2017. - 349 с.

Дополнительные рекомендации к дисциплине

1.Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Академия, 2009, 271 с.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. М.: Гелиос АРВ, 2002, 480 с.
3. Агибалов Г.П. Избранные теоремы начального курса криптографии : Учебное пособие. Томск: НТЛ, 2005, 116 с.
4. Мао Венбо. Современная криптография: теория и практика / Венбо Мао. М.: Издательский дом "Вильямс", 2005, 768 с.
5. Шнайер Брюс. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. М.: Триумф, 2002, 816 с.
6. Введение в криптографию / Под общ. ред. В.В. Ященко. – 4-е изд., доп. М.: МЦНМО, 2012, 348 с.
7. Кузьминов Т.В. Криптографические методы защиты информации / Т.В. Кузьминов. Новосибирск: Наука, 1998, 194 с.
8. Dan Boneh, Victor Shoup. A Graduate Course in Applied Cryptography. Publisher: Stanford University, 2017
9. Курс "Управление ключами шифрования и безопасность сети" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/553/409/info
10. Николенко С. Криптографические протоколы (видео) [Электронный ресурс] // Лекториум – академический образовательный проект . URL: https://www.lektorium.tv/lecture/26067

Б1.Б.1.16 Экономика
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	5 курс 9 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Зенкова Жанна Николаевна, к.ф.-м.н., доцент	Кафедра системного анализа и математического моделирования

Пререквизиты	Параллельно осваиваемые дисциплины
История, Философия, Социальная инженерия Математический анализ	Психология

Цель и задачи дисциплины

Цель: освоение базового материала об экономике, в том числе экономической теории, макро- и микроэкономике, методик расчётов показателей, связанных с экономической деятельностью и оценкой ее эффективности.

Задачи:

- рассмотреть государственное регулирование взаимодействия субъектов и последствия этого влияния на рынок потребителя;
- рассмотреть роль монополии и ее влияние на инфляционные процессы;
- рассмотреть способы расчета валового внутреннего продукта, его значимость в макроэкономических процессах;
- рассмотреть процессы, происходящие в рамках реальных предприятий РФ.

Результаты обучения	Методы обучения	Методы оценивания
Знать: содержание и взаимосвязь основных принципов, законов, понятий и категорий экономической теории, микро- и макроэкономики; основные методики расчета различных экономических показателей Уметь: рассчитывать и анализировать экономические показатели. Владеть: основными понятиями экономической науки, в том числе понятиями экономических ресурсов, спада и роста экономики, валового внутреннего продукта, инфляции; навыками расчета альтернативных (временных издержек).	• Лекции • Самостоятельная работа	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Введение в экономическую теорию	6					2	Изучение учебного материала.
Микроэкономика	14					20	Изучение учебного материала.
Макроэкономика	12					12	Изучение учебного материала.
Подготовка к прохождению промежуточной аттестации в форме зачета				1,6		4,15	
Прохождение промежуточной аттестации в форме зачета					0,25		

Всего	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	в конце семестра	Зачтено – знание и понимание материала, хотя бы на уровне общих представлений.

Литература

1. Максимова В.Ф. Экономическая теория: учебник для бакалавров: Учебник для бакалавров /Под общ. ред. Максимовой В.Ф. Эл. ресурс http://www.biblio-online.ru/book/ B3189507-C9B1-46E5-BF6E-2023D927FDD4, Юрайт, 2019. –580 с
2. Маховикова Г.А., Переверзева С.В. Микроэкономика. Продвинутый курс: учебник и практикум: Учебник и практикум. Эл. Ресурс http://www.biblio-online.ru/book/ 9742F44E-D272-4F7B-97B0-42FF7B3E461B, Юрайт, 2019. – 322 с.
3. Мёрфи Р. Уроки для молодого экономиста, Социум, 2019. – 483 с.
4. Боброва О.С., Цыбуков С.И., Бобров И.А. Организация коммерческой деятельности: учебник и практикум для СПО: Учебник и практикум. Эл. Ресурс http://www.biblio-online.ru/book/BE95C40C-7DD1-4F2D-97EB-C731C436DC6E, Юрайт, 2018. – 332 с.
5. Дорман В.Н., Кельчевская Н.Р. Экономика организации. Ресурсы коммерческой организации: учебное пособие для академического бакалавриата : Учебное пособие. Эл. ресурс http://www.biblio-online.ru/book/19BA664D-9438-48E1-8B1F-EA3DE74B28E8, Юрайт, 2018. – 134 с.
6. Зенкова Ж.Н. Учебные материалы для курса "Экономика": учебное пособие. Эл. ресурс: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000658710, ТГУ, 2019. – 42 с.
7. Родина Г.А., Тарасова С.В. Основы экономики. Микроэкономика: Учебник. Эл. ресурс http://www.biblio-online.ru/book/8D F212DD-3A12-4574-B702-D7B9B0C4B602, Юрайт, 2019. – 263 с.
8. Булатов А.С. Макроэкономика: Учебник. Эл. ресурс http://www.biblio-online.ru/book/7DB2 C9AF-BE01-4717-ACF6-CB5A74493C14, Юрайт, 2018. – 333 с.

Б1.Б.1.17 Правоведение
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	3 курс 6 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Туляй Екатерина Юрьевна, к.ю.н., доцент	Кафедра финансового права

Пререквизиты	Параллельно осваиваемые дисциплины
Иметь представление об основных отраслях российского права в объеме школьного курса обществознания	

Цель и задачи дисциплины

Цель: изучение и освоение студентами теории и истории государства и права, основ конституционного строя России, гражданского, трудового, семейного, уголовного, административного права и иных отраслей российского права.

Задачи:

- усвоение теоретических положений конституционного, гражданского, трудового, семейного, уголовного, административного права и иных отраслей российского права;
- выработка умений применять приобретенные знания на практике – в правоприменительной деятельности;
- обучение работе с документами – нормативно-правовыми актами и т.п.

Результаты обучения	Методы обучения	Методы оценивания
Знать: - основные положения и нормы конституционного, гражданского, трудового, семейного, уголовного, административного, финансового права, организацию судебных и правоохранительных и правоприменительных органов; - нормативные правовые акты в области защиты информации и государственной тайны; - правовые основы защиты государственной тайны; особенности правого регулирования будущей профессиональной деятельности. Уметь - защищать свои права, самостоятельно использовать знания об основах общей теории государства и права и базовые отрасли российского права в своей деятельности; - использовать нормативно-правовые знания в профессиональной деятельности.	• Лекции • Самостоятельная работа	• Зачет

Содержание дисциплины		
Темы занятий	**Контактные часы**	**Самостоятельная работа**

	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Понятие и сущность государства и права	2					6	Изучение учебного материала
Основы Конституционного права РФ	2					6	Изучение учебного материала, подготовка к занятиям
Трудовое право	2					6	Изучение учебного материала, подготовка к занятиям
Гражданское право	2					6	Изучение учебного материала, подготовка к занятиям
Уголовное и уголовно-процессуальное право	2					6	Изучение учебного материала, подготовка к занятиям
Административное право	2					6	Изучение учебного материала, подготовка к занятиям
Семейное право	2					6	Изучение учебного материала, подготовка к занятиям
Правовые основы защиты государственной тайны	2					6	Изучение учебного материала, подготовка к занятиям
Подготовка к прохождению промежуточной аттестации в форме зачета				0,8		6,95	
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего	16			0,8	0,25	54,95	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	в конце семестра	Зачтено – знание и понимание материала, хотя бы на уровне общих представлений.

Литература

1. Марченко М.Н., Дерябина Е.М. Правоведение: учебник для студентов неюридических вузов по курсу «Правоведение», М.: Проспект, 2008. – 416 с.

2. Правоведение: учебник для студентов вузов, обучающихся по специальности «Правоведение» / В.М. Шумилов, М.: Проспект, 2008. – 210 с.

Б1.Б.1.18 Основы управленческой деятельности
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	5 курс 10 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Дмитренко Анатолий Григорьевич, д.ф.-м.н., профессор	ИПМКН ,кафедра прикладной математики

Пререквизиты	Параллельно осваиваемые дисциплины
Правоведение, Экономика, Социальная инженерия	

Цель и задачи дисциплины

Цель: выработка у учащихся системного видения мира, системного и проектного мышления

Задачи:

- Ознакомить студентов с технологиями решения сложных проблем;
- Формирование умения «думать глобально, действовать локально»

Результаты обучения	Методы обучения	Методы оценивания
Уметь работать в коллективе; принимать управленческие решения в сфере профессиональной деятельности. Владеть навыком толерантного восприятия социальных, культурных и иных различий	• Лекции • Самостоятельная работа	• Реферат • Дискуссия • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Понятие прикладного системного анализа. Понятие системы. Понятие модели. Понятие управления	12					8	Изучение учебного материала. Обсуждение. Написание реферата
Фиксация проблемы. Составление списка участников проблемной ситуации. Составление проблемного месива	8					6	Изучение учебного материала. Дискуссия. Написание реферата
Выбор конфигуратора. Целевыявление. Выбор критериев. Экспериментальное исследование систем	8					8	Изучение учебного материала. Написание реферата
Проблемы построения и развития моделей. Генерирование альтернатив. Выбор (принятие решения). Теория системной практики	4					8	Изучение учебного материала. Дискуссия. Написание реферата
Подготовка к прохождению промежуточной аттестации в форме зачета				1,6		8,15	Подготовка к сдаче зачета
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100 %	В конце семестра	При проведении промежуточной аттестации в форме зачета, обучающемуся дается три вопроса. Зачтено ставится, если обучающийся ответил не менее, чем на два вопроса.

Литература

Тарасенко Ф.П. Прикладной системный анализ. – М.: КноРус, 2010.
Перегудов Ф.И., Тарасенко Ф.П. Введение в системный анализ. – М.:Высшая школа, 1989.

Б1.Б.1.19 Социальная инженерия
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	4 курс8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Беляев В.А., канд. тех. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины

Цель и задачи дисциплины

Цель – формирование знаний, необходимых для осуществления комплексного инженерного подхода к организации информационной безопасности предприятия с учётом социальной реальности.

Задачи: обеспечить приобретение знаний и умений необходимых для решения задач инженерно-технической защиты информации с учётом системного подхода.

Результаты обучения	Методы обучения	Методы оценивания
Овладение основами защиты интересов личности, общества и государства от возможных информационных атак, применением основных мер по ликвидации их последствий, способностью к общей оценке состояния информационной безопасности предприятия.	• Лекции • Самостоятельная работа	Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Введение. Социальная инженерия (СИ) как наука	2					2	Изучение учебного материала
Основные концептуальные положения СИ	2					2	Изучение учебного материала
История развития социальной инженерии	2					2	Изучение учебного материала
Информация как предмет защиты	2					2	Изучение учебного материала
Принципы и техники социальной инженерии	2					2	Изучение учебного материала
Основная модель социальной инженерии	2					2	Изучение учебного материала
Методы социальной инженерии	2					2	Изучение учебного материала
Основные направления социальной инженерной деятельности	2					2	Изучение учебного материала
Технологии социальной инженерии	2					2	Изучение учебного материала
Социальная инженерия и социальное	2					2	Изучение учебного материала

программирование							
Утечка корпоративной информации. Инсайдинг	2					2	Изучение учебного материала
Пределы последствий при социоинженерных атаках	2					2	Изучение учебного материала
Сопровождение социальных процессов в обществе	2					2	Изучение учебного материала
Технологии защиты от социальных «хакеров»	2					2	Изучение учебного материала
Комплексный подход к разработке политик информационной безопасности предприятия	4					2	Изучение учебного материала
Подготовка к зачету и прохождение промежуточной аттестации в форме зачета				1,6	0,25	8,15	
Всего:	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	**Зачтено**: студент владеет большей частью теоретического материала, но может иметь некоторые проблемы в знаниях, допускать негрубые ошибки; **Не зачтено**: студент не освоил большую часть теоретического материала.

Литература

1. Аполлонский А. В., Домбровская Л. А., Примакин А. И., Смирнова О. Г., Основы информационной безопасности в ОВД: Учебник для вузов. – СПб.: Университет МВД РФ, 2010.
2. Кевин Митник, Уильям Саймон — Призрак в Сети. Мемуары величайшего хакера. – М.: Издательство: «Эксмо», 2012. – 416 с..

Дополнительные рекомендации к дисциплине

1. Кузнецов М.В., Симдянов И.В. Социальная инженерия и социальные хакеры.-СПб: БХВ-Петербург, 2007. – 368 с.
2. Вильям Л. Саймон, К. Митник. Искусство обмана. -М: Компания АйТи, 2004. – 123 с.

Б1.Б.1.20 Психология
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	Специалитет	5 курс 9 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Бредун Екатерина Валерьевна, ассистент	Кафедра общей и педагогической психологии

Пререквизиты	Параллельно осваиваемые дисциплины
История, Философия, Правоведение	Экономика

Цель и задачи дисциплины

Цель дисциплины – обеспечить подготовку студентов в области освоения психологических знаний.
Задачи дисциплины: познакомить с теоретическими, экспериментальными и прикладными исследованиями в области психологии; изучить основные понятия, классификации, механизмы и закономерности психических процессов; сформировать представления о психологических механизмах, обеспечивающих оптимизацию организации эффективной учебной и профессиональной деятельности; развить навыки самостоятельного критического мышления.

Результаты обучения	Методы обучения	Методы оценивания
Знать основные морально-нравственные нормы общества. Уметь толерантно воспринимать культурные, этнические, конфессиональные, социальные и другие особенности. Владеть навыками определения и применения этических и морально-нравственных норм, принятых в обществе, основных принципов профессиональной этики.	• Лекции • Самостоятельная работа	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
История психологии	6					6	Изучение теоретического материала по теме
Познавательные процессы	6					6	Изучение теоретического материала по теме
Личность	6					6	Изучение теоретического материала по теме
Конструктивное общение	6					6	Изучение теоретического материала по теме
Психология групп	8					6	Изучение теоретического материала по теме
Подготовка к промежуточной аттестации				1,6		8,15	

в форме зачета							
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего:	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	**Зачтено**: студент владеет большей частью теоретического материала, но может иметь некоторые проблемы в знаниях, допускать негрубые ошибки; **Незачтено**: студент не освоил большую часть теоретического материала.

Литература
1. Клочко В.Е. Психология инновационного поведения [Электронный ресурс]/ «Российское образование» - Федеральный портал, URL: http://www.edu.ru/index.php?page_id=34
Дополнительные рекомендации к дисциплине
Научная электронная библиотека elibrary

Б1.Б.1.21 Математический анализ
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
24 з.е.	специалитет	1 курс 1, 2 семестр 2 курс 3, 4 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Воробейчиков Сергей Эрикович, д.ф.-м.н., доцент	Кафедра системного анализа и математического моделирования

Пререквизиты	Параллельно осваиваемые дисциплины

Цель и задачи дисциплины

Цель: изучение методов математического анализа, являющихся базовыми при изучении последующих дисциплин.

Задачи: освоить методы математического анализа, необходимые для решения прикладных задач в разных предметных областях

Результаты обучения	Методы обучения	Методы оценивания
Знать математический аппарат теории пределов функций, теории рядов; теории функциональных рядов; основные теоремы дифференциального и интегрального исчисления функций одного и нескольких переменных; понятие меры, измеримые функции и их свойства; абстрактный интеграл Лебега и его основные свойства. **Уметь** применять математический аппарат для решения профессиональных задач на основе вычислительной техники с привлечением математического аппарата теории пределов функций, дифференцирования, интегрирования и разложения функций в ряды. **Владеть** способностью самостоятельно применять аппарат математического анализа и вычислительной техники для решения профессиональных задач.	• Лекции • Практическая работа • Самостоятельная работа	• Экзамен • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен/Зачет	Часы СРС	Задания
1 семестр							
Действительные числа, пределы числовых последовательностей	32	32				20	Изучение учебного материала. Подготовка к практическим занятиям
Действительные функции действительной переменной	32	32				20	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к сдаче и сдача зачета				6,4	0,25	5,35	
Прохождение промежуточной аттестации в форме экзамена				2	0,3	33,7	
Итого	64	64		8,4	0,55	79,05	
2 семестр							
Интегральное исчисление функций	16	20				20	Изучение учебного материала.

действительной переменной. Вариация. Интегралы Римана, Стилтьеса							Подготовка к практическим занятиям
Основная теорема алгебры. Ряды с действительными и комплексными членами	18	20				10	Изучение учебного материала. Подготовка к практическим занятиям
n-мерные евклидовы пространства, функции нескольких переменных, предел и непрерывность. Ряд Тейлора	30	24				10	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к сдаче и сдача зачета				6,4	0,25	5,35	
Прохождение промежуточной аттестации в форме экзамена				2	0,3	33,7	
Итого	64	64		8,4	0,55	79,05	
3 семестр							
Дифференциальное исчисление функций нескольких переменных. Обратные отображения и неявные функции	12	12				20	Изучение учебного материала. Подготовка к практическим занятиям
Мера Жордана. Кратные интегралы. Интегралы, зависящие от параметра.	26	26				10	Изучение учебного материала. Подготовка к практическим занятиям
Теория поля. Криволинейные и поверхностные интегралы	26	26				10	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к сдаче и сдача зачета				6,4	0,25	6,35	
Прохождение промежуточной аттестации в форме экзамена				2	0,3	33,7	
Итого	64	64		8,4	0,55	79,05	
4 семестр							
Элементы теории Лебега и интегралы Лебега	20	20				10	Изучение учебного материала. Подготовка к практическим занятиям
Нормированные пространства и линейные функционалы	10	10				10	Изучение учебного материала. Подготовка к практическим занятиям
Функциональные ряды и интегралы Фурье	8	8				10	Изучение учебного материала. Подготовка к практическим занятиям
Дифференциальные уравнения	26	26				10	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к сдаче и сдача зачета				6,4	0,25	5,35	
Прохождение промежуточной аттестации в форме экзамена				2	0,3	33,7	
Итого	64	64		8,4	0,55	79,05	
Всего	256	256		33,6	2,2	316,2	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен, зачет	100, 100	В конце семестра	Уровень знания основных понятий и определения дисциплины; Уровень умения оперировать основными понятиями и определениями; вычислять пределы, производные, интегралы; решать обыкновенные дифференциальные уравнения. Уровень владения элементарными навыками применения основных понятий и определений; вычислений пределов, производных, интегралов; методами решений обыкновенных дифференциальных уравнений и систем.

Литература

1. Кудрявцев, Л. Д. Курс математического анализа в 3 т. Том 1 : учебник для бакалавров. М : Издательство Юрайт , 2019, 703 с.
2. Кудрявцев, Л. Д. Курс математического анализа в 3 т. Том 2 в 2 книгах. Книга 1 : учебник для бакалавров. М : Издательство Юрайт , 2018, 351 с.
3. Кудрявцев, Л. Д. Курс математического анализа в 3 т. Том 2 в 2 книгах. Книга 2 : учебник для бакалавров. М : Издательство Юрайт , 2017, 323 с.
4. Фихтенгольц Г.М. Основы математического анализа [Ч.] 1 : [учебник для вузов по направлениям подготовки и специальностям в области естественных наук и математики, техники и технологий, образования и педагогики] /Г.М. Фихтенгольц. - Санкт-Петербург: Лань, 2015. - 440 с.
5. Фихтенгольц Г.М. Основы математического анализа [Ч.] 2 : [учебник для вузов по направлениям подготовки и специальностям в области естественных наук и математики, техники и технологий, образования и педагогики] /Г.М. Фихтенгольц. - Санкт-Петербург: Лань, 2016. - 463 с.

Б1.Б.1.22 Геометрия
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
4 з.е.	специалитет	1 курс 2 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Тренькаев Вадим Николаевич, к.т.н., доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Для успешного освоения дисциплины обучающиеся должны обладать знаниями математики в пределах школьного курса	

Цель и задачи дисциплины

Цель: Сформировать способность корректно применять при решении профессиональных задач математический аппарат геометрии

Задачи:

- изучить основные понятия и задачи векторной алгебры;
- изучить аналитическую геометрию в пространстве.

Результаты обучения	Методы обучения	Методы оценивания
Знать основные понятия и задачи векторной алгебры и аналитической геометрии; методы аналитической геометрии для решения задач компьютерной безопасности. Уметь решать задачи векторной алгебры и аналитической геометрии.	• Лекции • Практические занятия • Самостоятельная работа	• Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Векторная алгебра	10	10				14	Изучение учебного материала. Подготовка к практическим занятиям
Аналитическая геометрия на плоскости	10	10				14	Изучение учебного материала. Подготовка к практическим занятиям
Аналитическая геометрия в пространстве	12	12				12,8	Изучение учебного материала. Подготовка к практическим занятиям
Индивидуальные консультации по дисциплине				3,2			
Прохождение промежуточной аттестации в форме экзамена				2	2,3	31,7	
Всего	32	32		5,2	2,3	72,5	

Оценивание

Вид работы	Удельный вес	Период	Критерии оценки
- Экзамен	100 %	В конце семестра	«Отлично» – демонстрация высокого уровня базовых знаний векторной алгебры и аналитической

			геометрии и умений выполнять стандартные действия, решать типовые задачи с учетом основных понятий, выбирать наиболее эффективные методы решения основных типов задач, владение навыками и приемами на высоком уровне. «Хорошо» – в целом успешное, но содержащее отдельные пробелы владение базовыми знаниями векторной алгебры и аналитической геометрии и умениями выполнять стандартные действия, решать типовые задачи с учетом основных понятий, выбирать наиболее эффективные методы решения основных типов задач. «Удовлетворительно» – частичное, фрагментарное владение базовыми знаниями векторной алгебры и аналитической геометрии и умениями выполнять стандартные действия, решать типовые задачи с учетом основных понятий, выбирать наиболее эффективные методы решения основных типов задач. «Неудовлетворительно» – обучающийся имеет существенные пробелы по отдельным теоретическим разделам дисциплины и демонстрирует низкий уровень владения базовыми знаниями векторной алгебры и аналитической геометрии и умениями выполнять стандартные действия, решать типовые задачи с учетом основных понятий.

Литература

1. Александров П. С. Лекции по аналитической геометрии: пополненные необходимыми сведениями из алгебры с приложением собрания задач, снабженных решениями, составленного А. С. Пархоменко /П. С. Александров Санкт-Петербург: Лань, 2016–911с
2. Беклемишев Д. В. Курс аналитической геометрии и линейной алгебры: учебник : [для студентов, изучающих курсы математики в классических университетах, а также технических вузах] /Д. В. Беклемишев. –Санкт-Петербург: Лань, 2015–244с.

http://e.lanbook.com/books/element.php?pl1_id=58162 Электронное издание Доступ к полному тексту документа после регистрации пользователя на сайте http://e.lanbook.com/ в локальной сети ТГУ

3. ПриваловИ. И. Аналитическая геометрия: учебник /И. И. Привалов–Санкт-Петербург: Лань, 2010–299с.

http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=321 Электронное издание Доступ к полному тексту документа после регистрации пользователя на сайте http://e.lanbook.com/ в локальной сети ТГУ

4. Клетеник Д. В. Сборник задач по аналитической геометрии /Д. В. Клетеник; под ред. Н. В. Ефимова Санкт-Петербург: Лань, 2010–222с.

http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=2044 Электронное издание Доступ к полному тексту документа после регистрации пользователя на сайте http://e.lanbook.com/ в локальной сети ТГУ

Б1.Б.1.23 Теория вероятностей и математическая статистика
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
9 з.е.	Специалитет	2 курс 4 семестр 3 курс 5 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Воробейчиков Сергей Эрикович, д.ф.-м.н., доцент	Кафедра системного анализа и математического моделирования

Пререквизиты	Параллельно осваиваемые дисциплины

Цель и задачи дисциплины

Цель – изучение аппарата теории вероятностей и его использования для решения задач в различных предметных областях.

Задача – освоить методы теории вероятностей, необходимые для решения прикладных задач, связанных с анализом свойств случайных событий и случайных величин; рассмотреть способы построения вероятностных моделей по данным наблюдений, а также способы проверки адекватности построенных моделей

Результаты обучения	Методы обучения	Методы оценивания
Владеть математическим аппаратом для решения задач в области теории вероятностей и математической статистики. **Уметь** применять современный математический аппарат при решении задач теории вероятностей и математической статистики. **Знать** современный математический аппарат для решения задач теории вероятностей и математической статистики.	• Лекции • Практические занятия • СРС	• Экзамен

Содержание дисциплины

Темы занятий	Контактные часы				Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Часы СРС	Задания
4 семестр						
Модели с конечным числом исходов. Классические модели и распределения.	2	2			4	Изучение учебного материала, подготовка к занятиям
Основные формулы для вероятностей событий. Теорема сложения вероятностей. Независимость случайных событий.	2	4			4	Изучение учебного материала, подготовка к занятиям

Условная вероятность события. Формула полной вероятности. Формула Байеса.						
Схема Бернулли. Закон больших чисел. Теоремы Муавра-Лапласа и Пуассона	4	4			4	Изучение учебного материала, подготовка к занятиям
Случайные величины как измеримые функции. Функция распределения случайной величины. Дискретные и непрерывные случайные величины. Плотность распределения вероятностей.	4	4			4	Изучение учебного материала, подготовка к занятиям
Числовые характеристики случайных величин.	4	6			4	Изучение учебного материала, подготовка к занятиям
Характеристическая функция и её свойства. Связь моментов случайной величины с её характеристической функцией	4	4			4	Изучение учебного материала, подготовка к занятиям
Условные математические ожидания, основные формулы.	4	2			4	Изучение учебного материала, подготовка к занятиям
Сходимость последовательностей случайных величин почти наверное, в среднем квадратическом, по вероятности, по распределению. Связь между различными типами сходимости.	4	4			4	Изучение учебного материала, подготовка к занятиям
Центральная предельная теорема. Условия Линдеберга и Ляпунова.	4	2			4	Изучение учебного материала, подготовка к занятиям
Закон больших чисел. Лемма Бореля-Кантелли. Усиленный закон больших чисел. Теоремы Колмогорова и Бореля	6	6			3	Изучение учебного материала, подготовка к занятиям
Случайные процессы. Пуассоновский процесс. Винеровский процесс. Марковские процессы.	10	10			4,2	
Подготовка к прохождению промежуточной аттестации в форме экзамена			4,8		33,7	
Прохождение промежуточной аттестации в форме экзамена			2	0,3		
Всего	48	48	6,8	0,3	76,9	
5 семестр						
Введение в математическую статистику. Элементы выборочной теории	4	4			6	Изучение учебного материала, подготовка к занятиям
Выборочные характеристики	4	4			6	Изучение учебного материала, подготовка к занятиям
Точечное оценивание параметров распределения	6	6			6	Изучение учебного материала, подготовка к занятиям
Свойства оценок параметров	4	4			6	Изучение учебного материала, подготовка к занятиям
Интервальное оценивание	4	4			6	Изучение учебного материала, подготовка к занятиям
Проверка статистических гипотез	6	6			6	Изучение учебного материала, подготовка к занятиям
Критерий Неймана-Пирсона. Критерий	4	4			4,8	Изучение учебного

Вальда						материала, подготовка к занятиям
Подготовка к прохождению промежуточной аттестации в форме экзамена			3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена			2	0,3		
Всего	32	32	5,2	0,3	74,5	
Итого	80	80	12	0,6	151,4	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100	В конце семестра	**Уровень знания** современных методов теории вероятностей и математической статистики и возможности их использования для решения прикладных задач **Уровень умения** находить способы решения задач, связанных с анализом случайных явлений. **Уровень владения** математическим аппаратом для решения задач в области теории вероятностей и математической статистики

Литература

1. Ширяев А.Н. Вероятность: в 2 кн: – М.: МЦНМО, 2011.
2. Боровков А.А. Теория вероятностей. – М.: ЛИБРОКОМ, 2014.
3. Прохоров А.В., Ушаков В.Г., Ушаков Н.Г. Задачи по теории вероятностей. – М.: КДУ, 2009.
4. Боровков А.А. Математическая статистика. - С-Пб.: Лань, 2016.

Ширяев А.Н. Задачи по теории вероятностей. – М.: МЦНМО, 2006

5. Ивченко Г.И., Медведев Ю.И., Чистяков А.В. Задачи с решениями по математической статистике – М.: Дрофа, 2007.
6. Ивченко Г.И., Медведев Ю.И. Введение в математическую статистику –М.: ЛКИ, 2010.

Б1.Б.1.24 Алгебра
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
22 з.е.	специалитет	1, 2 курс 1, 2, 3, 4 семестр 4 семестра	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Пахомова Елена Григорьевна, к.ф.-м.н, доцент Приходовский Михаил Анатольевич, к.ф.-м.н, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
нет	Математический анализ, Геометрия

Цель и задачи дисциплины

Цель:

- получение студентами теоретических знаний и формирование у них практических навыков по линейной алгебре, теории групп, теории колец, теории делимости, в частности, делимости целых чисел, делимости многочленов.

Задачи:

- изучить основы линейной алгебры: теорию решения систем линейных уравнений, фундаментальные понятия теории линейных пространств и линейных операторов.
- изучить основные алгебраические структуры: группы, кольца, поля
- дать понятие о задачах и методах теории целых и комплексных чисел, теории многочленов
- сформировать у студентов навык самостоятельного изучения учебной и научной литературы в области математики

Результаты обучения	Методы обучения	Методы оценивания
Обучающийся должен: • **знать:** базовую терминологию алгебры, основные понятия и теоремы дисциплины; основные свойства важнейших алгебраических структур (групп, колец, полей); основные алгоритмы алгебры (метод Гаусса, алгоритм Евклида, нахождение кратных корней многочлена, схема Горнера и т.д.); теорию конечных полей; • **уметь:** решать задачи теоретического и прикладного характера из различных разделов алгебры; • **владеть:** математическим аппаратом алгебры, методами доказательства утверждений в этой области; • **обладать следующими компетенциями, перечисленными в ООП**: ОПК-2.	• Лекции • Практические занятия	• Экзамены в 1, 2, 3 и 4 семестрах • Уровень выполнения контрольных работ

Содержание дисциплины							
Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
I семестр							
Основные алгебраические структуры	6	6				7,65	Изучение теоретического материала. Выполнение практических заданий
Матрицы и определители над коммутативным кольцом с 1	6	6				7,65	Изучение теоретического материала. Выполнение практических заданий
Матрицы над полем	4	6				5,1	Изучение теоретического материала. Выполнение практических заданий
Линейная зависимость векторов над полем	6	4				5,1	Изучение теоретического материала. Выполнение практических заданий
Системы линейных уравнений	12	12				15,3	Изучение теоретического материала. Выполнение практических заданий
Экзамен				2		33,7	Подготовка к сдаче экзамена
Всего за 1-й семестр	32	32		5,2		40,8	
II семестр							
Элементы теории множеств: множество, натуральные числа, принцип индукции, равномощность, сравнение множеств по мощностям, теорема Кантора-Бернштейна, счётные множества, несчётные множества, операции над мощностями, аксиомы теории множеств	8	8				5,8	Изучение теоретического материала. Выполнение практических заданий
Элементы комбинаторики: основные комбинаторные принципы; наборы, размещения и сочетания, биномиальная формула, биномиальные коэффициенты, числа Стирлинга, принцип включений и исключений, обращение Мёбиуса, подстановки на конечным множестве	8	8				5,8	Изучение теоретического материала. Выполнение практических заданий
Числовые системы: кольца целых чисел, классов вычетов целых чисел, целых р-адических чисел, поля рациональных, действительных и комплексных чисел, алгебра кватернионов	10	10				7	Изучение теоретического материала. Выполнение практических заданий
Арифметика целых чисел: деление с остатком, алгоритм Евклида и расширенный алгоритм Евклида, основная теорема арифметики, арифметика остатков	10	10				7	Изучение теоретического материала. Выполнение практических заданий
Многочлены над полем: деление с остатком, алгоритм Евклида и расширенный алгоритм Евклида, основная теорема арифметики, арифметика остатков, построение конечных полей	10	10				7	Изучение теоретического материала. Выполнение практических заданий
Корни многочленов: корни многочленов над целостным кольцом, теорема Безу, схема Горнера, методы	10	10				7	Изучение теоретического материала. Выполнение практических заданий

интерполяции, метод Кронекера разложения в конечное число шагов, полиномиальные функции над целостным кольцом							
Симметрические многочлены и результант: симметрические многочлены и основная теорема о симметрических многочленах, результант двух многочленов, симметрические функции корней, результант как симметрическая функция корней, дискриминант	8	8				5,8	Изучение теоретического материала. Выполнение практических заданий
Зачет					0,25		Подготовка к сдаче зачета
Экзамен				2		33,7	Подготовка к сдаче экзамена
Всего за 2-й семестр	64	64		8,4		45,35	
III семестр							
Основы теория групп: основные свойства операций, примеры групп, циклическая группа, нормальная подгруппа, фактор-группа, гомоморфизмы групп, прямые произведения групп, полупрямые произведения, свободные группы и свободные произведения, действие группы на множестве	52	52				36,85	Изучение теоретического материала. Выполнение практических заданий
Дополнительные разделы теории групп: нормальные и субнормальные ряды, нильпотентные и разрешимые группы, p-группы, теоремы Силова, группы малых порядков	12	12				8,5	Изучение теоретического материала. Выполнение практических заданий
Зачет					0,25		Подготовка к сдаче зачета
Экзамен				2		33,7	Подготовка к сдаче экзамена
Всего за 3-й семестр	64	64		8,4		45,35	
IV семестр							
Теория колец: основные свойства операций в кольце, основные примеры колец, подкольца и идеалы, факторкольцо, гомоморфизмы, прямые суммы и произведения, разложение в прямую сумму, разложение коммутативного кольца с единицей, китайская теорема об остатках	18	18				12,75	
Теория делимости в области целостности: простые и максимальные идеалы, отношения делимости и ассоциированности, простые и неприводимые элементы, область с разложением и с однозначным разложением, область главных идеалов, евклидова область целостности, нётерово кольцо, теорема Гильберта о базисе, теорема Гаусса о факториальности, признаки неприводимости	18	18				12,75	

(критерий Эйзенштейна и редукционный критерий)							
Теория полей: основные свойства операций в поле, основные примеры полей, расширение поля, степень расширения, конечные н алгебраические расширения, простое расширение, теорема о примитивном элементе, поле разложения многочлена, конечные поля (характеристика, порядок, существование и единственность, подполя, неприводимые многочлены)	18	18				12,75	
Модуль над кольцом с единицей: основные свойства операций, подмодуль, фактор-модуль, гомоморфизмы, прямые суммы и произведения, свободный модуль	10	10				7,1	
Зачет					0,25		Подготовка к сдаче зачета
Экзамен				2		33,7	Подготовка к сдаче экзамена
Всего за 4-й семестр	64	64		8,4		45,35	
Всего	**224**	**224**		**30,4**		**311,65**	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
- Зачет - Экзамен	Зачет – 20% Экзамен – 80%	В конце семестра	**Отлично**: знание и понимание материала в полном объеме. **Хорошо**: хорошее знание материала за исключением некоторых деталей. **Удовлетворительно:** не глубокое понимание материала, на уровне общих представлений.

Литература

- **Основная литература:**

1. Глухов М. М. Алгебра : [учебник для вузов по специальности "Информационная безопасность"] / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. - Изд. 2-е, испр. и доп.. - Санкт-Петербург [и др.] : Лань, 2015. - 606 с. - (Учебники для вузов. Специальная литература) . URL1: http://e.lanbook.com/books/element.php?pl1_id=67458
2. Курош А. Г. Курс высшей алгебры : [учебник для вузов по специальностям "Математика", "Прикладная математика"] / А. Г. Курош. - Изд. 19-е, стер.. - Санкт-Петербург [и др.] : Лань, 2013. - 431 с.: ил. - (Знание. Уверенность. Успех!) - (Лучшие классические учебники) - (Классическая учебная литература по математике) - (Учебники для вузов. Специальная литература)
3. Каргаполов М. И. Основы теории групп : учебное пособие / Каргаполов М. И., Мерзляков Ю. И.. - Изд. 5-е, стер.. - Санкт-Петербург [и др.] : Лань, 2009. - 287 с.: ил. - (Учебники для вузов. Специальная литература) . URL1: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=177
4. Курош А. Г. Теория групп : учебник / А. Г. Курош. - Изд. 4-е, стереотип.. - СПб. [и др.] : Лань, 2005. - 648 с.: ил. - (Лучшие классические учебники. Математика) . URL1: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=562
5. Варден Б. Л. Алгебра : [перевод] / Б. Л. ван дер Варден. - 3-е изд., стер.. - СПб. [и др.] : Лань, 2004. - 623 с. - (Учебники для вузов)

- **Дополнительная литература**

6. Ленг С. Алгебра / С. Ленг ; пер. с англ. Е. С. Голода ; под ред. А. И. Кострикина. - М. : Мир, 1968. - 564 с.: рис.
7. Кострикин А. И. Введение в алгебру : [учебник для университетов по специальностям "Математика" и "Прикладная математика"]. Ч. 1 / А. И. Кострикин. - Изд. 2-е, испр.. - Москва : Физматлит, 2004. - 271 с.
8. Кострикин А. И. Введение в алгебру : Учебник для университетов по специальностям "Математика" и "Прикладная математика". Ч. 2 / А. И. Кострикин. - М. : Физико-математическая литература, 2000. - 367, [1] с.: ил.
9. Кострикин А. И. Введение в алгебру : Учебник для университетов по специальностям "Математика" и "Прикладная математика". Ч. 3 / А. И. Кострикин. - М. : Физико-математическая литература, 2000. - 271, [1] с.: ил.
10. Фаддеев Д. К. Задачи по высшей алгебре : [учебное пособие для студентов вузов, обучающихся по математическим специальностям] / Д. К. Фаддеев, И. С. Соминский. - Изд. 17-е, стер.. - Санкт-Петербург : Лань, 2008. - 287, [1] с. - (Математика) - (Классическая учебная литература по математике) - (Знание. Уверенность. Успех!) - (Классические задачники и практикумы) - (Учебники для вузов. Специальная литература) . URL1: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=399
11. Икрамов Х. Д. Задачник по линейной алгебре : учебное пособие / Х. Д. Икрамов ; под ред. В. В. Воеводина. - Изд. 2-е испр.. - Санкт-Петербург : Лань, 2006. - 319, [1] с. - (Классические задачники и практикумы) - (Лучшие классические учебники. Математика) . URL1: http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=165
12. Крылов П. А. Задачи по теории колец, модулей и полей / П. А. Крылов, А. А. Туганбаев, А. Р. Чехлов. - М. : Факториал Пресс, 2007. - 240 с. - (Методы современной математики ;вып. 6:)

Дополнительные рекомендации к дисциплине

Базы данных и информационно-справочные системы, в том числе зарубежные

1. Михалев А., Михалев А. Алгебра матриц и линейные пространства // Национальный Открытый Университет «ИНТУИТ» – 2019. – URL: https://intuit.ru/studies/courses/992/207/info (дата обращения: 01.09.2019)
2. Михалев А., Михалев А. Введение в алгебру // Национальный Открытый Университет «ИНТУИТ» – 2019. – URL: https://intuit.ru/studies/courses/1009/197/info (дата обращения: 01.09.2019)
3. Чернова Н. Введение в линейную алгебру // Национальный Открытый Университет «ИНТУИТ» – 2019. – URL: https://intuit.ru/studies/courses/1016/208/info (дата обращения: 01.09.2019)
4. Головань С. Линейная алгебра // Национальный Открытый Университет «ИНТУИТ» – 2019. – URL: https://intuit.ru/studies/courses/616/472/info (дата обращения: 01.09.2019)
5. Чепуркин Константин. Алгебра // Просветительский проект «Лекториум» – 2019. - URL: https://www.lektorium.tv/node/38907 (дата обращения: 01.09.2019)
6. Карев М. Алгебра // Просветительский проект «Лекториум» – 2019. – URL: https://www.lektorium.tv/node/37328 (дата обращения: 01.09.2019)
7. Петров В. Алгебра // Просветительский проект «Лекториум» – 2019. – URL: https://www.lektorium.tv/course/28719 (дата обращения: 01.09.2019)
8. Вавилов Н. высшая алгебра // Просветительский проект «Лекториум» – 2019. – URL: https://www.lektorium.tv/course/26552 (дата обращения: 01.09.2019)

Б1.Б.1.25 Математическая логика и теория алгоритмов
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
4 з.е.	Бакалавриат	3 курс 6 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Галанова Н. Ю., к.ф.-м.н., доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Введение в математику Дискретная математика	Теория автоматов. Компьютерные сети. Теоретико-числовые методы в криптографии.

Цель и задачи дисциплины

Цель: сформировать способность корректно применять при решении профессиональных задач аппарат математической логики и теории алгоритмов (ОПК-2), сформировать способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).

Задачи: знать основные понятия математической логики, уметь анализировать математические доказательства средствами математической логики. Владеть основными теоретическими положениями логики высказываний, логики предикатов, теории алгоритмов.

Результаты обучения	Методы обучения	Методы оценивания
ОР-1. Знать язык логики нулевого порядка. Уметь доказывать Эквивалентность формул с помощью таблиц истинности и законов алгебры логики. Уметь применять алгоритмы приведения формулы к ДНФ, КНФ, СДНФ, СКНФ; проверки формулы на ТИ, ТЛ, алгоритмы проверки логического следования и связанные с ним, в том числе методом резолюций. Знать обоснование полноты метода резолюций, доказательство теоремы компактности. ОР-2. Знать понятия исчисления высказываний (секвенций): аксиомы и правила вывода, вывод. Уметь строить вывод формулы. Анализировать связь между исчислением высказываний и логикой высказываний. Разбираться в проблемах разрешимости, непротиворечивости, полноты и независимости для исчисления высказываний (секвенций). ОР-3. Владеть понятиями логики первого порядка (термы, формулы, интерпретация языка, общезначимость, логическое следование) Владеть алгоритмами приведения к Сколемовской нормальной форме, алгоритмами доказательства логического следования, доказательства общезначимости и др., в том числе методом резолюций. ОР-4. Иметь представление об исчислении предикатов. Знать примеры теорий первого порядка. ОР-5. Владеть алгоритмами элиминации кванторов в упорядоченном множестве рациональных чисел и др. ОР-6. Владеть понятиями: частично-рекурсивные, примитивно-рекурсивные, общерекурсивные функции. Анализировать и распознавать принадлежность функций к одному из этих типов. Иметь представление об алгоритмической вычислимости, тезисе Черча.	Лекции Практические занятия Самостоятельная групповая и индивидуальная работа	• Контрольные работы • ИДЗ • Экзамен .

Содержание дисциплины							
Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Логика нулевого порядка.	8	8		0,5		10	СР1. РКС СР2. КНФ, ДНФ, СКНФ, СДНФ СР3. Логическое следование СР4 Метод резолюций ИДЗ
Исчисление высказываний (секвенций).	4	4		0,5		10	СР5. Выводимость
Логика первого порядка (логика предикатов).	10	10		1		10,8	ДЗ СР6. Предикаты. СР7. ПНФ СР8. Логическое следование. СР9. Метод резолюций. Контрольная работа.
Исчисление предикатов.	2	2		0,5			ДЗ
Выразимость. Элиминация кванторов.	4	4		0,5		10	ДЗ СР10. Элиминация кванторов.
Рекурсивные функции.	4	4		0,2			ДЗ
Подготовка к прохождению промежуточной аттестации в форме экзамена						33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	32		5,2	0,3	74,5	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
СР1-5, ИДЗ	25%	В 1половине семестра	Полнота ответа на вопросы
Экзамен (Часть 1)	25%	В середине семестра	Полнота ответа на вопросы
СР6-10, ДЗ	25%	Во 2 половине семестра	Полнота ответа на вопросы
Экзамен(Часть 2)	25%	В конце семестра	Полнота ответа на вопросы

Литература

1. Глухов М.М., Козлитин О.А., Шапошников В.А., Шишков А.Б. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов. - СПб: Лань, 2021
2. Верещагин Н., Шень А. Языки и исчисления. МЦНМО. 2017. 240 с.
3. В.А. Романович. Лекции по математической логике. 4.1,2. Томский государственный университет. 2015.

Б1.Б.1.26 Дискретная математика
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
9 з.е.	специалитет	1 курс 1 семестр 2 курс 3 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Андреева Людмила Николаевна, канд. техн. наук, доцент; Широкова Екатерина Владимировна, ассистент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Нет	Б1.Б.1.24 Алгебра

Цель и задачи дисциплины

Цель: Познакомить студентов с основными понятиями теории множеств, теории графов, булевых функций и функций k-значной логики, а также научить использовать изученные методы дискретной математики для формализации и решения прикладных задач.

Задачи:

- Дать представление о теоретических основах современных информационных технологий.
- Научить пользоваться методами дискретной математики (в частности, методами комбинаторики, теории отношений, теории графов, математической логики) для формализации и решения прикладных задач.

Результаты обучения	Методы обучения	Методы оценивания
ОПК-2: Обучающийся будет **знать** проблемы минимизации и функциональной полноты булевых функций; **знать** основные понятия и теоремы теории графов, булевых функций и функций k-значной логики. **уметь** применять алгоритмы и теоремы булевых и k-значных функций и графов в задачах защиты информации. **ОПК-4:** Обучающийся будет **владеть** аппаратом функций булевых и k-значной логики и графов для задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования. **ОПК-10:** Обучающийся будет **уметь** самостоятельно программировать алгоритмы теории графов, булевых функций и функций k-значной логики в доверенном системном программном обеспечении; **владеть** доверенными системными и прикладными программными средствами реализации алгоритмов теории графов, булевых функций и функций k-значной логики.	• Аудиторные лекции • Практические занятия • Самостоятельная работа	• Контрольные работы • Экзамен

Содержание дисциплины							
Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
1 семестр							
Раздел 1. Основные понятия теории булевых функций	10	5		0,6		7	Изучение учебного материала; выполнение контрольных заданий
Раздел 2. Нормальные формы булевых функций	11	5		0,6		7	Изучение учебного материала; выполнение контрольных заданий
Раздел 3. Минимизация булевых функций	11	6		1		7	Изучение учебного материала; выполнение контрольных заданий
Раздел 4. Не полностью определенные булевы функции и системы булевых функций	11	5		0,8		7	Изучение учебного материала; выполнение контрольных заданий
Раздел 5. Важнейшие замкнутые классы и функциональная полнота	11	6		1		8	Изучение учебного материала; выполнение контрольных заданий
Раздел 6. Функции k-значной логики	10	5		0,8		7,2	Изучение учебного материала; выполнение контрольных заданий
Промежуточная аттестация в форме экзамена				2	0,3	33,7	Подготовка к сдаче экзамена
Итого	64	32		6,8	0,3	76,9	
3 семестр							
Раздел 1. Основы теории графов	10	10		0,8		20	Изучение учебного материала; выполнение контрольных заданий
Раздел 2. Оптимизационные задачи теории графов	22	22		1,2		20,8	Изучение учебного материала; выполнение контрольных заданий
Промежуточная аттестация в форме экзамена				2	0,3	33,7	Подготовка к сдаче экзамена
Итого	32	32		5,2	0,3	74,5	
ИТОГО	96	64		12	0,6	151,4	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100%	В сессию	Оценка «Отлично» - обучающийся уверенно владеет аппаратом булевых функций, функций k-значной логики и графов для задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования. Уверенно владеет навыками решения задач повышенной трудности, базовыми знаниями в дискретной математике (теории булевых функций). Оценка «Хорошо» - обучающийся хорошо владеет аппаратом булевых функций, функций k-значной логики и графов для задания структуры и поведения

			дискретных (цифровых) устройств, в частности, устройств шифрования. Хорошо владеет навыками решения задач, базовыми знаниями в дискретной математике (теории булевых функций). Оценка «Удовлетворительно» - обучающийся недостаточно владеет аппаратом булевых функций, функций k-значной логики и графов для задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования. Недостаточно владеет навыками решения задач, базовыми знаниями в дискретной математике (теории булевых функций). Оценка «Неудовлетворительно» - обучающийся не владеет аппаратом булевых функций, функций k-значной логики и графов для задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования. Не владеет навыками решения задач, базовыми знаниями в дискретной математике (теории булевых функций).

Литература

Перечень основной учебной литературы:

1. Яблонский С.В. Введение в дискретную математику. -М.: Высшая школа, 2010. - 381 с.
2. Быкова С.В., Буркатовская Ю.Б. Булевы функции. Учебное пособие, - Томск: ТГУ, - 2008. - 192 с.
3. Калугин Н.А., Калугин А.Н. Элементы теории графов. - Самара: Изд-во СГАУ, 2013. - 44 с.

Перечень ресурсов информационно-телекоммуникационной сети Интернет:

1. Издательство «Лань» [Электронный ресурс] : электрон.-библиотечная система. - Электрон. Дан. - СПб., 2010. - URL: htto://e.laubook.com/
2. ScienceDirect [Electronic resource] / Elsevier B.V. - Electronic data. - Amsterdam, Netherlands, 2016. -URL: http://www.sciencedirect.com/

Дополнительные рекомендации к дисциплине

Перечень дополнительной учебной литературы:

1. Закревский А. Д., Потгосин Ю. В., Черемисинова Л. Д. Основы логического проектирования. В 3 кн. Кн 2. - Мн.:ОИПИ ВАН Беларуси, 2004. - 240 с.
2. Конспект лекций О.Б.Лупанова по курсу «Введение в математическую логику» /Отв. ред. А.Б.Угольников. М.: Изд-во ЦПИ при механико-математическом факультете МГУ имени М.В.Ломоносова, 2007. - 192 с.
3. Емеличев В.А., Мельников О.И., Сарванов В.И., Тышкевич Р.И. Лекции по теории графов. - М.: Наука, 1990. - 384 с.
4. Харари Ф. Теория графов. М.: Мир, 1973. - 300 с.
5. Оре О. Теория графов. -М.: Наука, 1980. - 336 с.6.
6. Кристофидес Н. Теория графов. Алгоритмический подход. — М.: Мир, 1977.
7. Домнин Л.Н. Элементы теории графов: учебное пособие. — Пенза: Изд-во Пенз. гос. Ун-та, 2007. - 144 с.

Б1.Б.1.27 Дискретная математика. Теория автоматов
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
4 з.е.	специалитет	3 курс 6 семестр	Обязательная, входит в базовую часть	Очное обучение	Русский

Преподаватель	Структурное подразделение
Твардовский Александр Сергеевич, к.ф.-м.н., старший преподаватель	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Дискретная математика, Алгебра	Методы верификации, Аппаратная реализация криптоалгоритмов, Модели безопасности компьютерных систем

Цель и задачи дисциплины

Цель: изучить основные положения теории автоматов, связь конечно-автоматных моделей с регулярными языками и формальными грамматиками, эксперименты над автоматами и их структурный синтез.

Задачи:

- Изучить основные понятия теории автоматов.
- Изучить связь автоматов с регулярными языками.
- Изучить связь автоматов с формальными грамматиками.
- Изучить автоматы-преобразователи и эксперименты над ними.
- Изучить структурный синтез конечных автоматов.

Результаты обучения	Методы обучения	Методы оценивания
Знать основные понятия теории автоматов. **Уметь** использовать математический аппарат теории автоматов. **Владеть** навыками решения задач в области теории автоматов. **Знать** методы научных исследований в области теории автоматов. **Уметь** применять методы научных исследований в области теории автоматов. **Знать** методы разработки алгоритмов теории автоматов. **Владеть** навыками разработки алгоритмов теории автоматов.	• Лекции • Изучение учебного материала • Решение задач на практических занятиях	• Экзамен • Контрольные работы

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Автоматы и регулярные языки	6	6				8	Изучение учебного материала, подготовка к практическим занятиям
Автоматы и грамматики	6	6				8	Изучение учебного материала, подготовка к практическим занятиям
Автоматы-преобразователи	8	8				8	Изучение учебного материала, подготовка к практическим занятиям
Эксперименты с автоматами	6	6				8	Изучение учебного материала, подготовка к практическим занятиям

Структурный синтез конечных автоматов	6	6				8,8	Изучение учебного материала, подготовка к практическим занятиям
Индивидуальная консультация				3,2			
Подготовка к прохождению промежуточной аттестации в форме экзамена						33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	32		5,2	0,3	74,5	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Контрольные работы	20%	В течение семестра	Решено не менее 70% задач
Экзамен	80%	В конце семестра	Отлично – Сформированные систематические представления об основных понятиях теории автоматов и умение использовать математический аппарат теории автоматов. Владение навыками решения задач теории автоматов. Сформированные системные знания методов научных исследований и умение применять методы научных исследований в области теории автоматов. Сформированные системные знания методов разработки алгоритмов и умение разрабатывать алгоритмы теории автоматов. Хорошо – Сформированные, но содержащие отдельные пробелы, представления об основных понятиях теории автоматов и умение использовать математический аппарат теории автоматов. Хорошее владение навыками решения задач теории автоматов. Сформированные, но содержащие отдельные пробелы, знания методов научных исследований и умение применять методы научных исследований в области теории автоматов. Сформированные, но содержащие отдельные пробелы, знания методов разработки алгоритмов и умения разрабатывать алгоритмы теории автоматов. Удовлетворительно – Неполные представления об основных понятиях теории автоматов. В целом успешное, но не систематическое умение использовать математический аппарат теории автоматов. Удовлетворительное владение навыками решения задач теории автоматов. Общие, но не структурированные знания методов научных исследований. Частично успешно применяемые методы научных исследований в области теории автоматов. Общие, но не структурированные знания методов разработки алгоритмов. Частично освоенное умение разрабатывать алгоритмы теории автоматов. Неудовлетворительно – Непонимание основных понятий теории автоматов. Посредственное умение использовать математический аппарат теории автоматов. Фрагментарное владение навыками решения задач теории автоматов. Фрагментарные знания методов научных исследований. Не освоенные методы научных исследований в области

			теории автоматов. Фрагментарные знания методов разработки алгоритмов. Не освоенное умение разрабатывать алгоритмы теории автоматов.

Литература

1. Буркатовская Л. И. Логическое проектирование дискретных устройств : учебное пособие : [для студентов, изучающих историю автоматов] / Л. И. Буркатовская, Ю. Б. Буркатовская ; Том. гос. ун-т, Фак. прикладной мат. и кибернетики. - Томск : Том. гос. ун-т, 2011. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000418985
2. Хопкрофт Д. Э. Введение в теорию автоматов, языков и вычислений : Джон Хопкрофт, Раджив Мотвани, Джеффри Ульман ; [под ред. А. Б. Ставровского ; пер. с англ. О. И. Васылык и др.]. - 2-е изд.. - Москва [и др.] : Вильямс, 2008. - 1 онлайн-ресурс (528 с.): ил.. URL: http://sun.tsu.ru/limit/2017/000565917/000565917.pdf
3. Гилл А. Введение в теорию конечных автоматов / А. Гилл. – М. : Издательство Наука, 1966. – 272 с.
4. Сперанский Д. В. Лекции по теории экспериментов с конечными автоматами : учебное пособие : [для студентов и аспирантов математических и инженерных специальностей] / Д. В. Сперанский. - Москва : Интернет-Университет Информационных Технологий [и др.], 2012. - 287 с.: ил., табл. - (Основы информационных технологий)

Дополнительные рекомендации к дисциплине

1. Агибалов Г. П. Лекции по теории конечных автоматов. / Г. П. Агибалов, А. М. Оранов. – Томск : Издательство ТГУ, 1984. – 185 с.
2. Курс “Математика в тестировании дискретных систем”. URL: https://stepik.org/course/73866/info (дата обращения: 27.02.2022)
3. Карпов Ю. Г. Теория автоматов : учебник для вузов по направлению подготовки бакалавров "Информатика и вычислительная техника" и по специальности "Вычислительные машины, комплексы, системы и сети" направления подготовки дипломированных специалистов "Информатика и вычислительная техника" / Ю. Г. Карпов. - СПб. [и др.] : Питер, 2003. - 206 с.: ил. - (Учебник для вузов)

Б1.Б.1.28 Теория информации
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	4 курс 7 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Ерёмина Наталия Леонидовна, кандидат технических наук	Кафедра системного анализа и математического моделирования

Пререквизиты	Параллельно осваиваемые дисциплины
Информатика, Дискретная математика, Теория вероятностей и математическая статистика	Криптографические методы защиты информации

Цель и задачи дисциплины

Цель дисциплины: дать научно-теоретические основы для корректного построения математических моделей физических процессов системы передачи информации в источниках сообщений и каналах связи
Задачи дисциплины: усвоение основных положений информационного подхода к анализу и синтезу объектов, явлений и систем; введение в вероятностно-статистические модели системы передачи информации, усвоение ее аксиоматических положений и разработанных на их основе методов приема и передачи информации.

Результаты обучения	Результаты обучения	Результаты обучения
• Знать основы теории информации, методы эффективного и помехоустойчивого кодирования информации. • Уметь производить подсчет количества информации в сообщениях; кодировать цифровые данные. • Владеть методиками эффективного и помехоустойчивого кодирования.	• Лекции • Семинары • Решение задач	• Тест • Задание • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
1. Энтропия дискретных источников	6	2				11	Изучение учебного материала. Подготовка к практическим занятиям
2. Неравномерное кодирование дискретных источников	6	4				11	Изучение учебного материала. Подготовка к практическим занятиям
3. Кодирование дискретных источников при неизвестной статистике	6	4				11	Изучение учебного материала. Подготовка к практическим занятиям
4. Алгоритмы кодирования источников, применяемые в архиваторах	6	2				11	Изучение учебного материала. Подготовка к практическим занятиям
5. Кодирование для дискретных каналов с шумом	8	4				9,35	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка и сдача промежуточной аттестации в форме зачета				2,4	0,25	4	
Всего	32	16		2,4	0,25	57,35	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Тест 1	10	В течение семестра	7 и более баллов – зачтено Менее 7 баллов – не зачтено
Тест 2	10	В течение семестра	7 и более баллов – зачтено Менее 7 баллов – не зачтено
Задание 1	15	В течение семестра	Задание выполнено, на все вопросы по заданию даны ответы – зачтено Задание не выполнено, не на все вопросы даны ответы – не зачтено
Задание 2	15	В течение семестра	Задание выполнено, на все вопросы по заданию даны ответы – зачтено Задание не выполнено, не на все вопросы даны ответы – не зачтено
Зачет	50	В конце семестра	Дан ответ на оба вопроса билета

Литература

1. Галлагер Т. Теория информации и надежная связь. М.: «Советское радио», 1974. 720 с.
2. Кудряшов Б.Д. Теория информации. СПб: Питер, 2018. 320 с.

Б1.Б.1.29 Физика
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
9 з.е.	специалитет	3 курс 5, 6 семестр 4 курс 7 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Дмитренко Анатолий Григорьевич, доктор физ.-мат. наук, профессор кафедры прикладной математики	Кафедра прикладной математики

Пререквизиты	Параллельно осваиваемые дисциплины
Математический анализ, Алгебра, Теория вероятностей и математическая статистика	Научно-исследовательская работа

Цель и задачи дисциплины

Цель – привить навыки работы с учебной литературой по физике, обучить студентов основным физическим теориям и законам, умению пользоваться физическими законами при решении практических задач и разработке математических моделей технических систем.

Лекционный курс включает такие разделы как механика, колебания и волны, молекулярная физика и термодинамика, электростатика, магнитостатика, основы электродинамики, основы квантовой механики, строение атомов, зонную теорию твердых тел. Лекционный материал затем закрепляется путем решения задач по изучаемой теме на практических занятиях.

Результаты обучения	Методы обучения	Методы оценивания
Обучающийся сможет: - находить в учебной литературе по физике необходимую информацию относительно темы исследований; - критически оценивать найденную информацию; - выполнять стандартные действия с учетом основных понятий и общих закономерностей, формулируемых в рамках физики; - решать типовые задачи с учетом физических законов; - использовать основные понятия, концепции, принципы физики для решения практических задач, связанных с прикладной математикой и информатикой.	– лекции; –практические занятия;	– устные опросы; – контрольные работы; – домашние задания; – зачет, экзамен.

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен/Зачет	Часы СРС	Задания
5 семестр							
Раздел 1. Введение	8	4				14	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 2. Механика	8	4				14	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 3. Колебания и волны	8	4				14	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 4. Термодинамика и молекулярная физика	8	4				14	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Подготовка к зачету				2,4		1,35	

Прохождение промежуточной аттестации в форме зачета					0,25		
Итого	32	16		2,4	0,25	57,35	
6 семестр							
Раздел 5. Электростатика	8	4				14	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 6. Магнитостатика	8	4				14	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 7. Электромагнитные явления	8	4				14	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 8. Элементы релятивистской физики	8	4				14	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Подготовка к зачету				2,4		1,35	
Прохождение промежуточной аттестации в форме зачета					0,25		
Итого	32	16		2,4	0,25	57,35	
7 семестр							
Раздел 9. Геометрическая оптика	8	4				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 10. Волновая оптика	8	4				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 11. Квантовая оптика	8	4				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 12. Элементы квантовой механики	4	2				4	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Раздел 13. Зонная теория твердых тел	4	2				5,6	Изучение учебного материала, подготовка к практическим занятиям, выполнение домашних работ
Подготовка к экзамену				2,4		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Итого	32	16		4,4	0,3	55,3	
Всего	96	48		9,7	0,3	170	

<table>
<tr><th colspan="4">Оценивание</th></tr>
<tr><th>Вид работы</th><th>Удельный вес</th><th>Период</th><th>Критерии оценки</th></tr>
<tr><td>Устные опросы</td><td rowspan="2">52 %</td><td rowspan="3">В течение семестра</td><td rowspan="4">Текущий контроль успеваемости в течение семестра разделен на три блока: 1) три устных опроса каждого из студентов по группе наиболее существенных тем; 2) 2 контрольные работы; 3) выполнение домашних работ. Зачеты и экзамен проходят в форме собеседования с преподавателем, в результате которого определяется уровень знаний студента. Критерии оценивания доводятся до сведения обучающихся преподавателем в начале курса.</td></tr>
<tr><td>Контрольные работы</td></tr>
<tr><td>Домашние задания</td><td>21 %</td></tr>
<tr><td>Зачеты, экзамен</td><td>27 %</td><td>В конце каждого из семестров</td></tr>
<tr><td colspan="4">Литература</td></tr>
</table>

1. Трофимова Т.И. Физика: учебник / Т.И. Трофимова. – М.: Академия, 2016. – 315 с.
2. Никеров В.А. Физика. Современный курс: учебник / В.А. Никеров. – М.: Дашков и К, 2015. – 451 с.
3. Ливенцев Н.М. Курс физики: учебник / Н.М. Ливенцев. – СПб.: Лань, 2012. – 666 с.
4. Кузнецов С.И. Физика: механика, механические колебания и волны, молекулярная физика, термодинамика: учебное пособие / С.И. Кузнецов. – М.: Вузовский учебник, 2014. – 246 с.
5. Власов А.А. Макроскопическая электродинамика: учебное пособие / А.А. Власов. – М.: ЛИБРОКОМ, 2010. – 228 с.
6. Трофимова Т.И. Физика: справочник с примерами решения задач: учебное пособие / Т.И. Трофимова. – М.: Высшее образование, 2010. – 447 с.
7. Гладков Л.Л. Физика: практикум по решению задач: учебное пособие / Л.Л. Гладков, А.О. Зеневич, Ж.П. Лагутина, Т.В. Мацуганова. – СПб.: Лань, 2014. – 282 с.

Б1.Б.1.30 Информатика
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
11 з.е	магистратура	1 курс, 1,2 семестры	Обязательная	Очное обучение	Русский

Преподаватели	Структурное подразделение
Беляев Виктор Афанасьевич, к.т.н., доцент	Каф. компьютерной безопасности ИПМКН
Панкратова Ирина Анатольевна, к.ф.м.н., доцент	Каф. компьютерной безопасности ИПМКН

Пререквизиты	Параллельно осваиваемые дисциплины
нет	Дискретная математика

Цель и задачи дисциплины

Цель дисциплины

Семестр 1 - формирование у студентов первичных знаний об организации аппаратного обеспечения ЭВМ и разработка навыков процесса программирования.

Семестр 2 - становление алгоритмического мышления.

Задачи дисциплины

Семестр 1 - знакомство студентов с базовыми компонентами архитектуры ЭВМ и основами программирования.

Семестр 2 - рассмотреть теоретические основы информатики: алгоритмические системы (нормальные алгорифмы Маркова, машины Тьюринга и Поста, рекурсивные функции) и основы методов трансляции (Польская инверсная запись, теория формальных грамматик и языков)

Результаты обучения	Методы обучения	Методы оценивания
Знать: основные понятия теории алгоритмов, основные подходы к задаче трансляции. Уметь: записывать простейшие алгоритмы в различных алгоритмических системах; разрабатывать, реализовывать, отлаживать и оптимизировать алгоритмы. Владеть: навыками алгоритмического мышления	• Лекции • Практические занятия • Лабораторные работы в компьютерном классе	• Экзамены в 1 и 2 семестрах • Уровень выполнения контрольных работ

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен/Зачет с оценкой	Часы СРС	Задания
Семестр 1							
Раздел 1. Основы архитектуры ЭВМ	2					1	Изучение лекционного материала
Раздел 2. Структура и принципы функционирования центрального процессора	6					2	Изучение лекционного материала
Раздел 3. Подсистемы памяти	8					3	Изучение лекционного материала
Раздел 4. Базовые функциональные элементы ЭВМ	4					2	Изучение лекционного материала
Раздел 5. Подсистема управления	4					2	Изучение лекционного материала
Раздел 6. Подсистема ввода-вывода	2					2	Изучение лекционного материала
Раздел 7. Система прерываний	2					1	Изучение лекционного

							материала
Раздел 8. Периферийные устройства ЭВМ						4	Самостоятельное изучение учебного материала
Раздел 9. Общая организация ЭВМ						1	Самостоятельное изучение учебного материала
Раздел 10. Введение в алгоритмизацию	4					2	Изучение лекционного материала
Раздел 11. Синтаксис языка С++		14	14			7	Подготовка к практическим занятиям
						6	Выполнение контрольных работ
Раздел 12. Массивы		14	10			5	Подготовка к практическим занятиям
						5	Выполнение контрольных работ
Раздел 13. Строки		10	4			3	Подготовка к практическим занятиям
						3	Выполнение контрольных работ
Раздел 14. Побитовые операции		10	4			2,15	Подготовка к практическим занятиям
						2	Выполнение контрольных работ
Подготовка и прохождение промежуточной аттестации в форме зачета				5,6	0,25		
Подготовка к промежуточной аттестации в форме зачета с оценкой						6,75	
Прохождение промежуточной аттестации в форме зачета с оценкой.				2	0,25		
Всего за 1-й семестр	32	48	32	7,6	0,5	59,9	
Семестр 2							
Раздел 15. Основные понятая теории алгоритмов	2					4	Изучение лекционного материала
Раздел 16. Нормальные алгорифмы Маркова	1,5					4	Изучение лекционного материала
Раздел 17. Машины Тьюринга и Поста	1,5					4	Изучение лекционного материала
Раздел 18. Рекурсивные функции	6					6	Изучение лекционного материала
Раздел 19. Польская инверсная запись	2					4	Изучение лекционного материала
Раздел 20. Основы теории формальных грамматик	1					4	Изучение лекционного материала
Раздел 21. Работа с файлами		6	6			3	Подготовка к практическим занятиям
						3	Выполнение контрольных работ
Раздел 22. Простые алгоритмы поиска и сортировки		4	4			4	Подготовка к практическим занятиям
						3	Выполнение контрольных работ
Раздел 23. Структуры		6	6			4	Подготовка к практическим занятиям
						3	Выполнение контрольных работ
Раздел 24. Динамическая структура типа		6	6			3	Подготовка к практическим

список							занятиям
						3	Выполнение контрольных работ
Раздел 25. Стек, рекурсия		4	4			2	Подготовка к практическим занятиям
						2,15	Выполнение контрольных работ
Раздел 26. Польская инверсная запись		6	6			3	Подготовка к практическим занятиям
						3	Выполнение контрольных работ
Подготовка и прохождение промежуточной аттестации в форме зачета				5,6	0,25		
Подготовка к промежуточной аттестации в форме экзамена.						33,7	
Прохождение промежуточной аттестации в форме экзамена.				2	0,3		
Всего за 2-й семестр	32	48	32	7,6	0,55	95,85	
Всего за год	64	96	64	15,2	1,1	155,7	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
- Устный экзамен - Итоговая оценка по выполнению к/р	50 50	В конце 1-го и 2-го семестров В конце 1-го и 2-го семестров	Уровень усвоения лекционного материала Уровень навыков в разработке алгоритмов и их реализации

Литература

- **Основная литература:**

1. Симонович С.В. Информатика: базовый курс: [для бакалавров и специалистов: учебное пособие для студентов высших технических учебных заведений] /под ред. С. В. Симоновича. – СПб.: Питер, 2015. - 637 с.
2. Орлов С.А., Цилькер Б.Я. Организация ЭВМ и систем: [учебник для вузов по направлению "Информатика и вычислительная техника"]. - СПб.: Питер, 2015. - 685 с.
3. Новожилов О.П. Информатика: Учебник / О. П. Новожилов. - М.: Юрайт, 2016. 619 с.

- **Дополнительная литература:**

1. Канцедал, С. А. Алгоритмизация и программирование: учебное пособие /С. А. Канцедал. - Москва: Форум, 2017. - 351 с.
2. Таненбаум Э., Остин Т. Архитектура компьютера. - СПб.: Питер, 2015. 811 с.
3. Таненбаум Э., Бос Х. Современные операционные системы. - СПб.: Питер, 2017. 1119 с.

Дополнительные рекомендации к дисциплине

- **Перечень ресурсов информационно-телекоммуникационной сети Интернет.**

1. Головчинер М.Н. Информатика I. Введение в архитектуру ЭВМ: курс лекций. [Электронный ресурс]. - Томск: СДО «Электронный университет – Moodle». 2016. URL: https://moodle.tsu.ru/course/view.php?id=74108
2. Головчинер М.Н. Информатика II. Введение в операционные системы: курс лекций. [Электронный ресурс]. - Томск: СДО «Электронный университет – Moodle». 2016. URL: https://moodle.tsu.ru/course/view.php?id=7412
3. Трофимов В.В. Информатика в 2 т. Том 1: Учебник [Электронный ресурс] /Отв. ред. Трофимов В. В. - М.: Юрайт – 2016 -553с. URL: http://www.biblio-online.ru/book/9C6C2FF4-E481-4F40-A229-E7EE8CC10640

Б1.Б.1.31 Алгоритмы и структуры данных I
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е	специалитет	2 курс, 3семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Андреева Валентина Валерьевна, к.т.н, доцент	Кафедра компьютерной безопасности ИПМКН

Пререквизиты	Параллельно осваиваемые дисциплины
«Информатика», «Дискретная математика»	

Цель и задачи дисциплины

Цель дисциплины ознакомить студентов с базовыми структурами данных, методами и алгоритмами, обучить студентов применять известные методы для разработки эффективных алгоритмов решения поставленных практических задач.

Результаты обучения	Методы обучения	Методы оценивания
Знание основных языков программирования и основных методов разработки программ при решении прикладных задач.	• Лекции • Лабораторные работы	Контрольные работы Зачет с оценкой

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет с оценкой	Часы СРС	Задания
Этапы решения задачи с использованием ЭВМ	2					2	Изучение лекционного материала.
Анализ сложности алгоритмов.	3					2	Изучение лекционного материала.
Проработка этапов решения задач на примере решения задачи Коммивояжёра. Знакомство с понятием эвристические алгоритмы			3			2	Изучение методов. Подготовка к лабораторным работам.
Поиск данных в числовом массиве, в строке. БМ-поиск.	3					2	Изучение лекционного материала.
КМП-поиск.	3					2	Изучение лекционного материала.
Реализация алгоритма поиска подстроки в строке (БМ-поиск)			4			2	Изучение методов поиска. Подготовка к лабораторным работам.
Алгоритмы сортировки вставками	3					2	Изучение алгоритма.
Реализация алгоритма сортировки вставками.			4			2	Подготовка к лабораторным работам.
Алгоритмы сортировки выбором.	3					2	Изучение алгоритма.
Реализация алгоритма сортировки выбором.			4			2	Подготовка к лабораторным работам.
Алгоритмы обменной сортировки. Быстрый поиск Хоара.	3					2	Изучение методов обменной сортировки, проработка на конкретных примерах. Подготовка к лабораторным работам.

Реализация алгоритма обменной сортировки.			4			2	Изучение алгоритма.
Алгоритмы распределяющей сортировки.	3					2	Изучение алгоритма.
Алгоритмы сортировки слиянием.	3					2	Изучение алгоритма.
Рекуррентные соотношения.	3					2	Изучение материала.
Динамические структуры данных – списки.	3					2	Изучение материала.
Реализация задач с применением динамической структуры типа список.			4			2	Изучение материала.
Топологическая сортировка	3					2	Изучение алгоритма.
Реализация алгоритма топологической сортировки.			8			2,5	Изучение методов. Подготовка к лабораторным работам.
Индивидуальные консультации в семестре				3,2			
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего	32		32	3,2	0,25	40,55	

Оценивание			
Вид работы	**Удельный вес** (*в итоговой оценке, %*)	**Период**	**Критерии оценки**
1. Контрольная работа №1	20%	в течении семестра	Оценка контрольной работы, включающая теоретические и практические вопросы.
2. Контрольная работа №2	20%	в течении семестра	Оценка контрольной работы, включающая теоретические и практические вопросы.
3. Лабораторные работы	30%	в течении семестра	Реализация всех базовых методов.
4. Зачет с оценкой	20%	в конце семестра	Знание теоретического материала и умение реализовать изученные методы

Литература

Основная литература:

1. Дональд Э. Кнут; под общ. ред. Ю.В. Козаченко. Искусство программирования: Т. 1: Основные алгоритмы, 712 с. Изд. Вильямс 2012
2. Дональд Э. Кнут; под общ. ред. Ю.В. Козаченко. Искусство программирования: Т. 3: Сортировка и поиск, 822 с., Изд. Вильямс 2012
3. Дональд Э. Кнут; под общ. ред. Ю.В. Козаченко. Искусство программирования: Т. 4: Комбинаторные алгоритмы, 955 с., Изд. Вильямс 2013

Дополнительная литература

4. Вирт Н. Алгоритмы и структуры данных: с примерами на Паскале, 351 с., СПб.: Невский диалог, 2008.
5. Седжвик Р. Фундаментальные алгоритмы на C++. Части 1-4. Анализ. Структуры данных. Сортировка. Поиск, 688 с., Киев: ДиаСофт, 2001.

Дополнительные рекомендации к дисциплине

Лабораторные работы выполняется в интегрированной среде разработки Microsoft Visual Studio Community C++ 2017.

Базы данных и информационно-справочные системы, в том числе зарубежные

1. Издательство «Лань» [Электронный ресурс] : электрон.-библиотечная система. – Электрон. Дан. – СПб., 2010. – URL: http://e.lanbook.com/
2. ScienceDirect [Electronic resource] / Elsevier B.V. – Electronic data. – Amsterdam, Netherlands, 2016. – URL: http://www.sciencedirect.com/
3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. – Электрон. Дан. – М., 2000. – URL: http://elibrary/ru/defaultx.asp?

Б1.Б.1.32 Аппаратные средства вычислительной техники
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	2 курс3 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Беляев В.А., канд. тех. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины

Цель и задачи дисциплины

Цель – ознакомление обучающихся с устройством современного компьютера, конструктивными особенностями, принципом действия, характеристиками и эксплуатационными параметрами основных элементов и узлов ВТ и периферийного оборудования.

Задачи: обеспечить приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействовать формированию научного мировоззрения и системного мышления при разработке сложных цифровых устройств.

Результаты обучения	Методы обучения	Методы оценивания
Овладение знаниями и основными понятиями в области принципов работы цифровой электроники, математическими моделями и базовыми элементами цифровых схем, перспективами развития вычислительной техники	• Лекции • Самостоятельная работа	Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Принципы построения, работы и взаимодействия элементов и узлов ЭВМ	2					3	Изучение учебного материала
Архитектура ЭВМ. Сравнение архитектур ЭВМ разных поколений	2					3	Изучение учебного материала
Функциональные элементы и узлы ЭВМ. Комплексы элементов ЭВМ.	2					3	Изучение учебного материала
Структура центральной части ЭВМ. Организация и иерархическая структура памяти ЭВМ.	4					3	Изучение учебного материала
Периферийные устройства ЭВМ: накопители на МД и ОД, дисплеи, принтеры, сканеры, дигитайзеры, плоттеры, клавиатура, мышь.	2					3	Изучение учебного материала
Понятие микропроцессора и микропроцессорной системы. Поколения МП и их основные характеристики. Виды и технологии производства МП.	2					3	Изучение учебного материала

Принципы построения микропроцессорных систем. Интерфейсы МП систем.	2					3	Изучение учебного материала
Рабочие станции и серверы.	2					3	Изучение учебного материала
Архитектура персональных ЭВМ. Структура и принципы функционирования основных модулей. Вопросы проектирования ПЭВМ.	4					3	Изучение учебного материала
Архитектура мини- и универсальных ЭВМ. Способы повышения надежности системы информационной безопасности.	4					3	Изучение учебного материала
Архитектура, ориентированная на программное обеспечение. Объектно-ориентированная архитектура. Машины баз данных	4					3	Изучение учебного материала
Проблемы и перспективы развития вычислительной техники.	2					3	Изучение учебного материала
Подготовка к зачету и прохождение промежуточной аттестации в форме зачета				1,6	0,25	2,15	
Всего:	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	**Зачтено**: студент владеет большей частью теоретического материала, но может иметь некоторые проблемы в знаниях, допускать негрубые ошибки; **Не зачтено**: студент не освоил большую часть теоретического материала.

Литература

1. Бройдо В.Л. Архитектура ЭВМ и систем: учеб. / В.Л. Бройдо, О.П. Ильина - СПб. Питер, 2009 – 720 с.
2. Гук М. Аппаратные средства IBM PC: энцикл. – СПб.: Питер, 2003 – 923 с.
3. Гук М.Ю. Аппаратные средства IBM PC. Энциклопедия. - 3-е изд. - Изд. Питер, 2011.
4. Колдаев Архитектура ЭВМ: Учебное пособие / ЭБС ZNANIUM - Москва: Издательский Дом "ФОРУМ", 2010. – 384 с.
4. Максимов Архитектура ЭВМ и вычислительных систем: Учебник / ЭБС ZNANIUM - Москва: Издательство "ФОРУМ", 2010. – 512 с.
5. Таненбаум Э. Архитектура компьютера: Пер. с англ. / Э. Таненбаум, Т. Остин -СПб.: Питер, 2011. – 816 с.

Дополнительные рекомендации к дисциплине

1. www.studfiles.ru/preview/5368345/
2. www.rsl.in – российская научная библиотека.
3. www.computerra.uro – журнал о компьютерах «Компьютера»

Б1.Б.1.33 Компьютерные сети
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
4 з.е.	магистратура	3 курс 6 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Сущенко Сергей Петрович, д-р. техн. наук, профессор	Институт прикладной математики и компьютерных наук, кафедра прикладной информатики

Пререквизиты	Параллельно осваиваемые дисциплины

Цель и задачи дисциплины

Цель дисциплины – обучить студентов принципам организации компьютерных сетей, сетевых технологий и протоколов.
Задачи дисциплины: привить студентам навыки применения теории компьютерных сетей при проектировании сетей масштаба предприятия и настройке сетевых протоколов и сервисов.

Результаты обучения	Методы обучения	Методы оценивания
Обладает необходимыми знаниями основных концепций современных вычислительных систем. Использует методы высокопроизводительных вычислительных технологий, современного программного обеспечения, в том числе отечественного происхождения. Использует инструментальные средства высокопроизводительных вычислений в научной и практической деятельности.	• Лекции	• Тесты • Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
1. Основы компьютерных сетей	6					8	Изучение теоретического материала по теме 1.
2. Технологии физического уровня	6					8	Изучение теоретического материала по теме 2.
4. Управление информационным каналом	6					8	Изучение теоретического материала по теме 3.
5. Технологии построения локальных сетей	12					8	Изучение теоретического материала 4.
6. Уровень сетевого протокола	6					8	Изучение теоретического материала 5.
7. Уровень транспортного протокола	6					8	Изучение теоретического материала 6.
8. Структура прикладного уровня и совместное функционирование протоколов верхних уровней	6					9,6	Изучение теоретического материала 7.
Подготовка к промежуточной аттестации				2,4		33,7	
Прохождение промежуточной аттестации				2	0,3		
Всего:	48			4,4	0,3	91,3	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100%	В конце семестра	**Отлично**: студент полностью владеет теоретическим материалом; **Хорошо**: студент полностью владеет теоретическим материалом, но допускает ошибки или неточности; **Удовлетворительно**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает негрубые ошибки; **Неудовлетворительно**: студент не освоил большую часть теоретического материала.

Литература
Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2001.
Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2007.

Б1.Б.1.34 Защита в операционных системах
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	5 курс семестр А	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Брославский Олег Викторович, ассистент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
• Языки программирования; • Операционные системы; • Криптографические методы защиты информации	

Цель и задачи дисциплины

Цель: теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий построения защищенных ОС, а также средств и методов обеспечения защиты информации в ОС.

Задачи:

- изучение понятийного аппарата и общих подходов к обеспечению ИБ операционных систем;
- изучение средств и методов управления доступом в защищенных ОС;
- изучение средств и методов интеграции защищенных ОС в защищенную сеть.

Результаты обучения	Методы обучения	Методы оценивания
Знать: • средства и методы хранения и передачи аутентификационной информации • требования к подсистеме аудита и политике аудита; • защитные механизмы и средства обеспечения безопасности операционных систем; Уметь: • формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; • осуществлять меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты. Владеть: • навыками оценки уровня защиты операционных систем; • навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.	• Лекции • Практические занятия • Лабораторные работы	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы	Самостоятельная работа

	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Тема 1. Понятие защищенной операционной системы		2				11	Изучение учебного материала.
Тема 2. Управление доступом		8	4			11	Изучение учебного материала. Выполнение лабораторных работ
Тема 3. Идентификация, аутентификация и авторизация		8	4			11	Изучение учебного материала. Выполнение лабораторных работ
Тема 4. Аудит		8	4			11	Изучение учебного материала. Выполнение лабораторных работ
Тема 5. Интеграция защищенных операционных систем в защищенную сеть		6	4			11	Изучение учебного материала. Выполнение лабораторных работ
				2,65		2,35	Подготовка к сдаче зачета
Всего		32	16	2,65		57,35	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Лабораторные работы	50	В течение семестра	Корректность выполнения лабораторной работы. Понимание использованных подходов и технологий.
Зачет	50	В конце семестра	Полнота ответа на вопросы экзаменатора

Литература

- Бэндл Дэвид. Защита и безопасность в сетях Linux. Питер, 2002
- Проскурин В.Г. Защита в операционных система. Учебное пособие. Горячая линия Телеком, 2016

Дополнительные рекомендации к дисциплине

- Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие. Горячая линия Телеком, 2016
- Furgel, I., & Saftig, V. (2016). Common Criteria Protection Profile “Multiple Independent Levels Of Security: Operating System” [V2.03]. https://doi.org/10.5281/zenodo.51582

Б1.Б.1.35 Основы построения защищённых компьютерных сетей
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
6 з.е.	специалитет	4 курс 7, 8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Колегов Денис Николаевич, к.т.н., доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Введение в специальность, Компьютерные сети	Операционные системы

Цель и задачи дисциплины

Цель: познакомить студентов с основными классическим сетевыми атаками; рассмотреть основные протоколы, технологии и механизмы защиты от сетевых атак.

Задачи:

- изучить сетевые атаки: ARP Spoofing, MAC Flooding, MAC Spoofing, VLAN Hopping, ГР Spoofing, TCP Hijacking, DoS- и DDoS-атаки.
- рассматреть основные протоколы, технологии и механизмы защиты от сетевых атак: VPN, ШР5, Firewall, Proxy, Load Balancing, Post Security.
- рассмотреть технологии анализа защищенности компьютерных сетей: идентификация устройств, идентификация открытых портов, идентификация сетевых служб и программного обеспечения, уязвимостей.

Результаты обучения	Методы обучения	Методы оценивания
Уметь: формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях. **Знать:** механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня, защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений; **Владеть**: средствами инструментального анализа защищенности компьютерных сетей; основными средствами анализа защищенности компьютерных сетей; средствами построения защищенных компьютерных сетей.	• Лекции • Лабораторные занятия • Самостоятельная работа	• Зачет с оценкой • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет с оценкой/Зачет	Часы СРС	Задания
7 семестр							
Защита от атак канального уровня	2		2			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Защита коммутации	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Технология VPN	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям

Защита от атак DoS н DDoS	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Защита маршрутизации	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Защита транспортного уровня	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Защита сетевых устройств	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Технологии межсетевого экранирования	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Методы н технологии обнаружения вторжений	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Сканирование защищенности сетей	3		3			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Дизайн защищенных сетей	3		3			7,8	Изучение учебного материала. Подготовка к лабораторным занятиям
Индивидуальные консультации по дисциплине				3,2			
Прохождение промежуточной аттестации в форме зачета с оценкой				2	0,25	6,75	
Итого	32		32	5,2	0,25	74,55	
8 семестр							
Защита от атак канального уровня			3			3	Подготовка к лабораторным занятиям
Защита коммутации			3			3	Подготовка к лабораторным занятиям
Технология VPN			3			3	Подготовка к лабораторным занятиям
Защита от атак DoS н DDoS			3			3	Подготовка к лабораторным занятиям
Защита маршрутизации			3			3	Подготовка к лабораторным занятиям
Защита транспортного уровня			3			3	Подготовка к лабораторным занятиям
Защита сетевых устройств			3			3	Подготовка к лабораторным занятиям
Технологии межсетевого экранирования			3			3	Подготовка к лабораторным занятиям
Методы н технологии обнаружения вторжений			3			3	Подготовка к лабораторным занятиям
Сканирование защищенности сетей			3			3	Подготовка к лабораторным занятиям
Дизайн защищенных сетей			2			3	Подготовка к лабораторным занятиям
Подготовка и сдача промежуточной аттестации в форме зачета				1,6	0,25	5,15	
Итого			32	1,6	0,25	38,15	
Всего	32		64	7,05	0,25	112,7	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет с оценкой Зачет	100%	В конце семестра	Отлично – в совершенстве умеет формулировать и настраивать политику безопасности основных ОС, а также локальных КС, построенных на их основе; знает механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня, обеспечения сетевой безопасности. Владеет в совершенстве средствами инструментального анализа защищенности компьютерных сетей Хорошо – умеет формулировать и настраивать политику безопасности основных ОС, а также локальных КС, построенных на их основе; знает механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня, защитные механизмы и средства; уверенно владеет средствами инструментального анализа защищенности компьютерных

			сетей обеспечения сетевой безопасности Удовлетворительно – умеет формулировать и настраивать политику безопасности основных ОС; посредственно владеет средствами инструментального анализа защищенности компьютерных сетей Неудовлетворительно – не умеет формулировать и настраивать политику безопасности основных ОС, не знает механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровня; не владеет средствами инструментального анализа защищенности компьютерных сетей. Зачтено – знание теоретического материала и умение реализовать изученные методы Незачтено – незнание большей части теоретического материала и неумение реализовать изученные методы

Литература

1. W. Richard Stevens, Kevin R. Fall. TCP/IP Illustrated, Volume 1: The Protocols (2nd edition), 2012. Addison Wesley.
2. Sean Convery. Network Security Architectures. -ISBN-13: 978-1587142970. Перечень дополнительной учебной литературы:
3. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учеб, пособие. М.: Издательский центр «Академия», 2009. 272 с.

Дополнительные рекомендации к дисциплине

1. Cisco Network Security Baseline. - URL:
http://www.cisco.com/c/en/us/td/docs/solutions/Enteiprise/Security/BaseUne_Security/seciirebas ebook.html.
2. Cisco SAFE reference Guide. - URL:
http://www.cisco.coш/c/en/us/td/docs/solutions/Enteфrise/Security/SAFE_RG/SAFE_rg.htшl
3. TCP-IP Guide. - URL: http://www.tcpipguide.com/

Перечень информационных технологий, используемых при осуществлении образовательного процесса, включая программное обеспечение, информационные справочные системы — Cisco Packet Tracer, GNS3, VirtualBox, VMWare Player, Metasploit, Metasploitable 2/3, Kali Linux.

Б1.Б.1.36 Основы построения защищённых баз данных
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	4 курс 8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Головчинер Михаил Наумович, к.т.н., доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Системы управления базами данных	Основы построения защищенных компьютерных сетей

Цель и задачи дисциплины

Цель: Обучение студентов принципам обеспечения безопасности информации в автоматизированных информационных системах (АИС)

Задачи:

- приобретение системного подхода к проблеме защиты информации в СУБД;
- изучение моделей и механизмов защиты в СУБД.

Результаты обучения	Методы обучения	Методы оценивания
Освоение современных критериев и стандартов для анализа безопасности информационных систем на базе СУБД.	• Лекции	• Тест • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Раздел 1. **Теоретические основы безопасности в БД** Тема 1. Безопасность БД, угрозы, защита Тема 2. Критерии защищенности БД	4 2 2					2	Изучение учебного материала.
Раздел 2. Средства и методы обеспечения безопасности БД Тема 3. Модели безопасности в СУБД Тема 4. Целостность БД и способы ее обеспечения Тема 5. Транзакции и блокировки Тема 6. Ссылочная целостность Тема 7. Классификация угроз конфиденциальности СУБД Тема 8. Средства идентификации и аутентификации	24 2 2 2 2 2 2					16	Изучение учебного материала.

Тема 9. Средства управления доступом Тема 10. Аудит и подотчетность Тема 11. Средства, поддерживающие высокую готовность Тема 12. Распознавание вторжений в БД	2 2 2 2						
Раздел 3. Проектирование безопасных БД Тема 13. Основные понятия проектирования безопасных БД Тема 14. Классификация и типы моделей «клиент–сервер» в системах баз данных Тема 15. Распределенные базы данных Тема 16. Защита данных в распределенных системах	8 2 2 2 2					4	
						16.15	Подготовка к сдаче зачета
Всего	32			1,85		38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Вид оцениваемой работы: - Тест - Зачет	 50 % 50 %	В конце семестра	 Правильные ответы на 70% вопросов Ответ на билет на оценку «удовлетворительно»

Литература

1. Пригонюк Н.Д. Основы построения защищенных баз данных: Учебное пособие. /Н.Д. Пригонюк, В.И. Петров. — Воронеж: ООО «МИР», 2019. — 76 с. — URL: https://tversu.ru/sveden/files/Osnovy_postroeniya_zaschischennyh_baz_dannyh_10.05.01_MMZI.pdf / (дата обращения: 24.02.2022).
2. Защита информации в базах данных и экспертных системах: пособие для студентов фак. радиофизики и комп. технологий / В. В. Скакун. – Минск: БГУ, 2015. – 140 с. - URL: https://elib.bsu.by/bitstream/123456789/48524/5/%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B0%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8%20%D0%B2%20%D0%91%D0%94.pdf / (дата обращения: 24.02.2022).

Дополнительные рекомендации к дисциплине

Б1.Б.1.37 Защита программ и данных
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	5 курс 9 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Брославский Олег Викторович, ассистент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
• Языки программирования; • Операционные системы;	

Цель и задачи дисциплины

Цель: теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий; формирование у обучающегося компетенций для научно-исследовательского и эксплуатационного видов деятельности.

Задачи:

- сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;
- участие в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте;
- разработка математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность объектов; установка, наладка, тестирование и обслуживание аппаратно-программных средств обеспечения информационной безопасности компьютерных систем;
- установка, наладка, тестирование и обслуживание системного и прикладного программного обеспечения;
- проведение аттестации технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности или профилям защиты.

Результаты обучения	Методы обучения	Методы оценивания
Знать: • средства и методы хранения и передачи авторизованной информации; • требования к подсистеме аудита и политике аудита; • защитные механизмы и средства обеспечения безопасности программ и данных; Уметь: • осуществлять анализ программного обеспечения на наличия уязвимостей; • проводить дизассемблирование и отладку программного обеспечения противодействовать компьютерным атакам и вирусам с использованием антивирусного программного обеспечения. Владеть: • навыками оценки уровня защиты программ и данных.	• Практические занятия • Самостоятельная работа	• Зачет

Содержание дисциплины							
Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Тема 1. Анализ программных реализаций		10				10	Изучение учебного материала. Выполнение практических заданий
Тема 2. Защита программ от изучения		10				10	Изучение учебного материала. Выполнение практических заданий
Тема 3. Программные закладки		4				4	Изучение учебного материала. Выполнение практических заданий
Тема 4. Внедрение программных закладок		4				4	Изучение учебного материала. Выполнение практических заданий
Тема 5. Противодействие программным закладкам		4				4	Изучение учебного материала. Выполнение практических заданий
				1,85		6,15	Подготовка к сдаче зачета
Всего		32		1,85		38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Практические задания	50	В течение семестра	Корректность выполнения задания. Понимание использованных подходов и технологий.
Зачет	50	В конце семестра	Полнота ответа на вопросы экзаменатора

Литература

- Защита программ и данных, Учебное пособие, Проскурин, В. Г., 2011
- Программирование на языке ассемблера NASM для ОС Unix, Учебное пособие, Столяров А.В., 2011

Дополнительные рекомендации к дисциплине

- Reverse Engineering для начинающих, Юричев, Д., Электронный ресурс https://beginners.re/main.html

Б1.Б.1.38 Теоретико-числовые методы в криптографии
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
10 з.е.	специалитет	3 курс 6 семестр 4 курс 7 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Останин Сергей Александрович, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Дискретная математика Алгебра Введение в математику Алгоритмы и структуры данных I, II	Математическая логика и теория алгоритмов Дискретная математика. Теория автоматов Булевы функции в криптографии

Цель и задачи дисциплины

Цель: овладеть алгоритмами работы с большими числами, алгоритмами полиномиальной арифметики, методами решения теоретико- числовых задач в криптографии

Задачи:

- исследовать алгоритмы над большими числами, полиномами;
- Исследовать алгоритмы генерации простых чисел, факторизации и дискретного логарифмирования

Результаты обучения	Методы обучения	Методы оценивания
Формирование у студентов профессиональных компетенций в соответствии с ФГОС ВО по специальности *Компьютерная безопасность* путём привития им знаний теоретико-числовых методов в криптографии и умения применять их в профессиональной деятельности.	• Лекции • Видеолекции • Лабораторные занятия	• Тест • Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Семестр 6							
Алгоритмы работы с большими числами	12		12			25	Изучение учебного материала. Подготовка к лабораторным занятиям
Тесты на простоту и методы генерации простых чисел	10		10			25	Изучение учебного материала. Подготовка к лабораторным занятиям
Методы факторизации чисел	10		10			26,8	Изучение учебного материала. Подготовка к лабораторным занятиям
Подготовка к промежуточной аттестации в форме экзамена				3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32		32	5,2	0,3	110,5	
Семестр 7							
Дискретное логарифмирование в	16		16			38	Изучение учебного материала.

конечных циклических группах							Подготовка к лабораторным занятиям
Алгоритмы над полиномами: тесты на неприводимость, примитивность, факторизация полиномов	16		16			38,8	Изучение учебного материала. Подготовка к лабораторным занятиям
Подготовка к промежуточной аттестации в форме экзамена				3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32		32	5,2	0,3	110,5	
Итого	64		64	10,4	0,6	221	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
- Проект -	30	В течение семестра	Полнота ответов на вопросы
- Тест -	30		Правильные ответы на большую часть вопросов
- Экзамен -	40	В конце семестра	**Отлично**: знание и понимание материала в полном объеме. **Хорошо**: хорошее знание материала за исключением некоторых деталей. **Удовлетворительно:** не глубокое понимание материала, на уровне общих представлений. **Неудовлетворительно**: незнание материала, даже на уровне общих представлений

Литература

1. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.
2. *Белов А.Г.* Исследование алгоритма дискретного логарифмирования Адлемана // Вестник Томского госуниверситета. Приложение. 2005. № 14. С. 45 - 49.
3. *Белов А.Г., Панкратова И.А.* Сравнительный анализ двух генераторов простых чисел // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 77 - 80.
4. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2002.
5. Введение в криптографию ./Под. ред. Ященко В.В. М.: МЦНМО - ЧеРо, 1998.
6. *Земор Ж.* Курс криптографии. М.-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2006.
7. *Кнут Д.* Искусство программирования для ЭВМ. Том 2. Получисленные алгоритмы. М.: Мир, 1977.
8. *Коблиц Н.* Курс теории чисел и криптографии. М.: Научное изд-во ТВП, 2001.
9. *Маховенко Е.Б.* Математические основы криптографии (конспект лекций). С.-Пб.: изд- во СПбГТУ, 1999.
10. *Маховенко Е.Б.* Теоретико-числовые методы в криптографии. М.: Гелиос АРВ, 2006.
11. *Миллер Г.Л.* Гипотеза Римана и способы проверки простоты чисел // Кибернетический сборник, выл. 23, 1986. С. 31 - 50.
12. *Ноден П., КиттеК.* Алгебраическая алгоритмика. М.: Мир, 1999.
13. *Панкратова ИА.* Теоретико-числовые задачи в криптографии. Томск: РИО ТГУ, 2010.
14. *Панкратова И.А.* Теоретико-числовые методы в криптографии. Томск: РИО ТГУ, 2009.
15. *УильямсХ.* Проверка чисел на простоту с помощью вычислительных машин // Кибернетический сборник, вып. 23, 1986. С. 51 - 99.
16. *Фергюсон Н., Шнайер Б.* Практическая криптография. М.-С.-Пб.-Киев: Диалектика, 2005.
17. *Харин Ю.С., Берник В.И, Матвеев Г.В., Агиевин С.В.* Математические и компьютерные основы криптологии. Минск: Новое знание, 2003.
18. *Черёмушкин А.В.* Вычисления в алгебре и теории чисел. Курс лекций. М., 2002.
19. *Черёмушкин А.В.* Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002.
20. *Menezes A.J., Van Oorshot PC., Vanstone S.A.* Handbook of Applied Cryptography. N. Y.: CRC Press Series on Discrete Mathematics and Its Applications, 1997.

Б1.Б.1.39 Сети и системы передачи информации
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
4 з.е.	специалитет	5 курс 10 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Останин Сергей Александрович, к.т.н., доцент	кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Компьютерные сети	

Цель и задачи дисциплины

Цель: изучить основы ключевых технологий передачи данных, применяемых в современных сетях, изучить нижний уровень сетевой модели - физический уровень. Он определяет электрические, временные и прочие характеристики сетей, по которым биты информации пересылаются в форме электрических сигналов.

Задачи:

– рассмотреть теоретические основы передачи данных;

– рассмотреть три типа сред передачи – проводниковые (медный провод и оптоволокно), радиоэфир (наземная радиосвязь) и радиоэфир, связанный со спутниковыми системами;

– рассмотреть три примера систем связи, которые используются на практике в глобальных сетях: телефонная система (стационарная), мобильная телефонная система, кабельное телевидение.

Результаты обучения	Методы обучения	Методы оценивания
Знать: основные законы теории колебаний и волн, оптики; основные протоколы, механизмы и алгоритмы. **Уметь**: строить математические модели физических явлений и процессов; анализировать математические модели физических явлений и процессов; формулировать и настраивать политику безопасности локальных компьютерных сетей. **Владеть**: методами построения математических моделей физических явлений и процессов; методами проектирования сетей.	• Лекции • Практические занятия • Самостоятельная работа	• Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Линии связи Теоретические основы передачи данных. Спектр, затухание, волновое сопротивление. Проводные линии связи. Типы кабелей: витая пара, коаксиальный. Оптические линии связи. Световоды. Оптические кабели.	6	6				6	Изучение учебного материала. Подготовка к практическим занятиям
Аппаратура связи Устройство оптических приемопередатчиков. Лазеры.	6	6				6	Изучение учебного материала. Подготовка к практическим занятиям

Светодиоды. Лазерные диоды. Способы модуляции. Оптические усилители. Фотодетекторы. Разъемы							
Беспроводная связь Электромагнитный спектр. Радиосвязь. Связь в микроволновом диапазоне. Связь в инфракрасном и видимом диапазонах. Спутники связи	8	8				6	Изучение учебного материала. Подготовка к практическим занятиям
Цифровая модуляция и мульти-плексирование. Низкочастотная передача. Передача в полосе пропускания Частотное уплотнение. Мультиплексирование с разделением времени. Кодовое разделение каналов	2	2				6	Изучение учебного материала. Подготовка к практическим занятиям
Структура телефонной системы Местные линии связи: модемы, ADSL, беспроводная связь. Магистрали и мультиплексирование. Коммутация	6	6				6	Изучение учебного материала. Подготовка к практическим занятиям
Мобильная телефонная система Мобильные телефоны первого поколения: аналоговая передача. Второе поколение мобильных телефонов: цифровая передача голоса (G2). Мобильные телефоны третьего поколения: цифровая речь и данные	2	2				6	Изучение учебного материала. Подготовка к практическим занятиям
Кабельное телевидение Абонентское телевидение Кабельный интернет Распределение частот. Кабельные модемы	2	2				4,8	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к сдаче экзамена				3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	32		5,2	0,3	74,5	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100 %	В конце семестра	Должны быть сданы обязательные практические задания, иначе оценка "Неудовлетворительно". **Отлично**: студент полностью владеет теоретическим материалом; **Хорошо**: студент полностью владеет теоретическим материалом, но допускает ошибки или неточности; **Удовлетворительно**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает ошибки; **Неудовлетворительно**: студент не сдал обязательные практические задания и/или не освоил большую часть теоретического материала.

Литература

Основная литература
1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. - Спб.: Питер. 2006. – 958 с.
2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – СПб.: Питер, 2012. – 960 с.

Дополнительная литература

1. Уайндер С. Справочник по технологиям и средствам связи. – М.: Мир, 2000.

2. Радиотехнические системы передачи информации /Под ред. В.В. Калмыкова.– М.: Радио и связь, 1990.

3. Беллами Дж. Цифровая телефония. – М.: Радио и связь, 1986.

4. Гаранин М.В., Журавлев В.И., Кунегин С.В. Системы и сети передачи информации: Учебное пособие для вузов [Электронный ресурс]. – URL: http://eknigi.org/nauka_i_ucheba/52252-sistemy-i-seti-peredachi-informacii-uchebnoe.html

Дополнительные рекомендации к дисциплине

1. Электронный учебник по компьютерным сетям. Автор/создатель: Министерство Российской Федерации по атомной энергии Белоярский политехнический колледж [Электронный ресурс]. – URL: http://kafvt.narod.ni/Osia/frameset.htm

Б1.Б.1.40 Аппаратная реализация криптоалгоритмов
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	5 курс 9 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Языки программирования, Дискретная математика, Теория автоматов, Профессиональный перевод специальной литературы, Электроника и схемотехника, Криптографические методы защиты информации, Аппаратные средства вычислительной техники	Техническая защита информации Криптографические протоколы Постквантовая криптография

Цель и задачи дисциплины

Цель: формирование профессиональных компетенций в области аппаратных средств защиты информации, ознакомление с этапами проектирования цифровых устройств на ПЛИС.

Задачи:

- дать представление об этапах проектирования цифровых устройств на базе ПЛИС;
- дать представление об особенностях аппаратной реализации криптографических алгоритмах;
- ознакомить с современными инструментами автоматизированного проектирования.

Результаты обучения	Методы обучения	Методы оценивания
В результате изучения дисциплины студент должен **знать:** - основы проектирования цифровых устройств на базе ПЛИС **уметь:** - описывать поведение криптосистем на языке VHDL **владеть:** - инструментами автоматизированного проектирования цифровых устройств на базе ПЛИС	• Лекции • Лабораторные занятия	• Зачет с оценкой

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет с оценкой	Часы СРС	Задания
Основы технологии ПЛИС	4		4			4	Изучение учебного материала. Подготовка к лабораторным занятиям
Основы проектирования цифровых устройств	4		4			4	Изучение учебного материала. Подготовка к лабораторным занятиям
Язык описания аппаратуры VHDL	6		6			6	Изучение учебного материала. Подготовка к лабораторным

							занятиям
САПР ISE WebPACK	4		4			4	Изучение учебного материала. Подготовка к лабораторным занятиям
Аппаратные средства защиты информации на базе ПЛИС	14		14			13,8	Изучение учебного материала. Подготовка к лабораторным занятиям
Подготовка к зачету с оценкой				3,2		6,75	
Прохождение промежуточной аттестации в форме зачета с оценкой				2	0,25		
Всего	32		32	5,2	0,25	38,55	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет с оценкой	100%	В конце семестра	Отлично – студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях. Хорошо – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях. Удовлетворительно – студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении заданий на лабораторных занятиях. Неудовлетворительно – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении заданий на лабораторных занятиях.

Литература

1. Ушенина, И. В. Проектирование цифровых устройств на ПЛИС : учебное пособие / И. В. Ушенина. - Санкт-Петербург : Лань, 2019. - 408 с.
2. Пухальский Г.И. Проектирование цифровых устройств : учебное пособие / Г.И. Пухальский, Т. Я. Новосельцева. – СПб.: Лань, 2012 – 888 с.
3. Соловьев В.В. Архитектуры ПЛИС фирмы Xilinx: CPLD и FPGA 7-й серии / В.В. Соловьев – М.: Горячая линия - Телеком, 2016. – 392 с.

Дополнительные рекомендации к дисциплине

1.Тарасов И.Е. Разработка цифровых устройств на основе ПЛИС Xilinx с применением языка VHDL / И.Е.Тарасов. – М.: Горячая линия - Телеком, 2005. – 253 с.
2. Угрюмов Е.П. Цифровая схемотехника: Учеб. пособие для вузов / Е.П. Угрюмов. – 3-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2010. – 800 с.
3. Бибило П.Н. Основы языка VHDL: Учебное пособие / П.Н. Бибило. – Изд. 5-е. – М.: Книжный дом «ЛИБРОКОМ», 2012. – 328 с.
4. Поляков А.К. Языки VHDL и VERILOG в проектировании цифровой аппаратуры / А.К. Поляков. – М.: СОЛОН-Пресс, 2003. – 305 с.
5. Панасенко С.П. Алгоритмы шифрования. Специальный справочник/ С.П. Панасенко.– СПб.: БХВ-

Петербург, 2009 – 576 с.
6. Тренькаев В. Н. Аппаратная реализация криптографических алгоритмов : учебно-методический комплекс : [для студентов высших учебных заведений, обучающихся по направлению 10.05.01 «Компьютерная безопасность»] / Тренькаев В. Н. ; Том. гос. ун-т, [Ин-т дистанционного образования]. - Томск : [ИДО ТГУ], 2015. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000516087
7. Пономарев О. Г. Плис-технологии в радиофизике : лабораторный практикум / Пономарев О. Г. - Томск, 2011. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000421575
8. Буркатовская Л. И. Логическое проектирование дискретных устройств : учебное пособие : [для студентов, изучающих историю автоматов] / Л. И. Буркатовская, Ю. Б. Буркатовская ; Том. гос. ун-т, Фак. прикладной мат. и кибернетики. - Томск : Том. гос. ун-т, 2011. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000418985
9. Курс “Введение в цифровую схемотехнику ” [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/104/104/info

Б1.Б.1.41 Алгоритмы и структуры данных II
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
7 з.е.	специалитет	2 курс 2 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Голубева Ольга Ивановна, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Алгоритмы и структуры данных II Информатика Языки программирования Дискретная математика	Языки программирования Дискретная математика

Цель и задачи дисциплины

Цель:

Знакомство с базовыми структурами данных, методами и алгоритмами, применяемыми в программировании. Наработка навыков построения новых алгоритмов, их сравнительного анализа.

Задачи:

- Изучение методов внешней сортировки последовательностей чисел (файловые сортировки);
- изучение структуры данных – деревья, приемов и методов работы с ними; изучение методов построения и выполнения операций с деревьями, построения бинарных деревьев, деревьев поиска, сбалансированных деревьев поиска, оптимальных деревьев поиска;
- изучение методов сжатия данных с использованием кодирования;
- изучение методов хеширования данных;
- изучение работы с большими числами и алгоритмов выполнения основных арифметических операций над ними;
- программирование основных изученных методов.

Результаты обучения	Методы обучения	Методы оценивания
В (ОПК-2) – I **Владеть** навыками работы в современных информационных системах автоматического поиска для получения необходимой информации. У (ОПК-2) – I **Уметь** находить и использовать web-ресурсы. З (ОПК-3) –II **Знать** базовые структуры данных: массивы и списки, синтаксис и семантику алгоритмических конструкций языка программирования С++ высокого уровня. У (ПК-5) – I **Уметь** осуществлять поиск информации о новейших достижениях по информатике в сети «Интернет». В (ПК-7) – I **Владеть** методами разработки алгоритмических и программных решений. У (ПК-7) – I **Уметь** применять методы разработки алгоритмических и программных решений. З (ПК-7) – I **Знать** методы разработки алгоритмических и программных решений. Обучающийся должен: **знать**: базовые структуры данных, методы и алгоритмы, применяемыми в программировании; вычислительные алгоритмы, реализующие основные арифметические действия над большими числами, особенности их программной реализации; основные критерии оценки программных реализаций; **уметь**: программно реализовывать на языках высокого уровня основные алгоритмы файловых сортировок, операции над	• Лекции • Практические занятия • Лабораторные занятия	• Экзамен / Коллоквиумы • Лабораторные работы

деревьями, алгоритмы сжатия данных с использованием кодирования, алгоритмы хэширования данных, выполнения арифметических операций над большими числами; использовать языки и системы программирования для реализации и исследования алгоритмов; отлаживать программы; разрабатывать вычислительные алгоритмы. **владеть**: методами программной реализации алгоритмов; навыками проведения компьютерных экспериментов; методикой отладки, оптимизации и оценки программы; методами построения вычислительных алгоритмов; **обладать следующими компетенциями, перечисленными в ООП:** ОПК-2, ОПК-10, ПСК-1.2, ПСК-2.1.		

Содержание дисциплины							
Темы занятий	**Контактные часы**					**Самостоятельная работа**	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Тема 1. Алгоритмы внешней сортировки.	8	2				8	Изучение учебного материала.
Тема 2. Структура данных – деревья и алгоритмы работы с ними.							
2.1. Двоичные деревья.	4	2	4			4	Изучение учебного материала. Подготовка к лабораторным занятиям.
2.2. Деревья поиска.	4	2	6			4	Изучение учебного материала. Подготовка к лабораторным занятиям.
2.3. АВЛ-деревья.	4	2	6			4	Изучение учебного материала. Подготовка к лабораторным занятиям.
2.4. Оптимальные деревья поиска.	4	2				4	Изучение учебного материала.
2.5. Красно-черные деревья.	2					8	Изучение учебного материала.
2.6. Б-деревья.	2					4	Изучение учебного материала.
Тема 3. Алгоритмы кодирования и сжатия информации.	2	1				4	Изучение учебного материала.
Тема 4. Методы хеширования.	2	1				4	Изучение учебного материала.
Большие числа. Представление больших чисел, ввод и вывод, сравнение больших чисел. Написание основы класса «Большие числа» на языке C++ (конструкторы, деструктор, операции ввода и вывода, присваивания, сравнения и др.).		8	12			8	Изучение учебного материала. Подготовка к лабораторным занятиям.
Изучение алгоритмов выполнения арифметических операций сложения и вычитания над большими числами. Реализация аддитивных операций над большими числами.		4	8			4	Изучение учебного материала. Подготовка к лабораторным занятиям.
Изучение алгоритма выполнения		2	4			5,6	Изучение учебного материала.

арифметической операции умножения над большими числами. Реализация операции умножения больших чисел.							Подготовка к лабораторным занятиям.
Изучение алгоритмов выполнения арифметической операции деления над большими числами. Реализация операции деления больших чисел.		6	14			20	Изучение учебного материала. Подготовка к лабораторным занятиям.
Тестирование программы, реализующей работу с большими числами.			10				Подготовка к лабораторным занятиям.
Индивидуальные консультации в семестре				6,4			
Подготовка к сдаче экзамена						33,7	Подготовка к сдаче экзамена
Сдача экзамена				2	0,3		
Всего	32	32	64	8,4	0,3	115,3	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Вид оцениваемой работы: - Лабораторные работы - Экзамен/Коллоквиумы	 60% 40%	 в течение семестра в конце семестра	Определен набор лабораторных работ, которые необходимо выполнить для получения оценок 3, 4 и 5. Оценка за каждую лабораторную работу осуществляется в форме «Зачтено» или «Не зачтено». «Зачтено» ставится в том случае, если лабораторная работа выполнена (возможно, с замечаниями). В противном случае ставится «Не зачтено». Оценки на отдельные вопросы при проведении экзамена формируются следующим образом: 2 – не ответил на вопрос; 3 – ответил на вопрос, но с серьезными замечаниями; 4 – ответил на вопрос с небольшими замечаниями; 5 – уверенно и правильно ответил на вопрос.

Литература

1. Кнут Д. Э. Искусство программирования : [учебное пособие : пер. с англ.] / Дональд Э. Кнут ; под общ. ред. Ю. В. Козаченко. – 3-е изд. – М. [и др.] : Вильямс, 2012. – 712 с. – Т. 1 : Основные алгоритмы
2. Кнут Д.Э. Искусство программирования : [учебное пособие : пер. с англ.]. Т. 2. Получисленные алгоритмы. / Дональд Э. Кнут; под общ. ред. Ю. В. Козаченко. – 3-е издание. – Москва : Вильямс, 2012. – 828 с.
3. Кнут Д. Э. Искусство программирования : [пер. с англ.] / Дональд Э. Кнут ; под общ. ред. Ю. В. Козаченко. – 2-е изд. – М. [и др.] : Вильямс, 2012. – 822 с. – Т. 3 : Сортировка и поиск
4. Кнут Д. Э. Искусство программирования : [пер. с англ.] / Дональд Э. Кнут. – М. [и др.] : Вильямс, 2013. – 955 с. – Т. 4, А : Комбинаторные алгоритмы

Дополнительные рекомендации к дисциплине

1. Вирт Н. Алгоритмы и структуры данных : с примерами на Паскале / Никлаус Вирт ; [пер. с англ. Д. Б. Подшивалова]. – СПб. : Невский диалог, 2008. – 351 с.
2. Мейер Б. Методы программирования : [в 2-х т.]. Т. 2 / Б. Мейер, К. Бодуэн ; пер. с фр. Ю. А. Первина ; под ред. А. П. Ершова. - М. : Мир, 1982. - 368 с.
3. Сибуя М. Алгоритмы обработки данных / М. Сибуя, Т. Ямамото; Пер. с яп. Э. К. Николаевой; Под ред. В. В. Панферова. - М. : Мир, 1986. - 218,[6] с.: ил.
4. Гудман С. Введение в разработку и анализ алгоритмов / С. Гудман, С. Хидетниеми ; пер. с англ. Ю. Б. Котова [и др.] ; под ред. В. В. Мартынюка. - М. : Мир, 1981. - 366 с.: ил.
5. Дейкстра Э. Дисциплина программирования / Э. Дейкстра ; пер. с англ. И. Х. Зусман и др. ; под ред. Э. З. Любимского. - М. : Мир, 1978. - 274 с. - (Математическое обеспечение ЭВМ).

Б1.Б.2.01 Методы верификации
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
4 з.е.	специалитет	5 курс 9 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Шабалдина Наталия Владимировна, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Б1.Б.1.25 «Математическая логика и теория алгоритмов», Б1.Б.1.27 «Дискретная математика. Теория автоматов», Б1.Б.1.31 «Алгоритмы и структуры данных I», Б1.Б.1.41 «Алгоритмы и структуры данных II»	Б1.Б.2.02 «Безопасность веб-приложений»

Цель и задачи дисциплины

Цель: научить студентов осуществлять верификацию программ, в том числе, анализировать корректность реализаций алгоритмов защиты информации

Задачи:

1. Научить студентов применять формальные модели для описания поведения дискретных систем и взаимодействующих процессов (компонент), подбирать подходящую модель в зависимости от особенностей дискретной системы.
2. Научить студентов верификации на основе конечно-автоматной модели.
3. Научить студентов осуществлять формальную верификацию программ методом проверки на модели (model checking).

Результаты обучения	Методы обучения	Методы оценивания
ОР-1.1 Понимает важность формальной верификации программ **ОР-2.1** Умеет применять формальные модели для описания поведения дискретных систем и взаимодействующих процессов (компонент), подбирать подходящую модель в зависимости от особенностей дискретной системы. **ОР-2.2** Умеет выбирать подходящую модель неисправности для тестирования дискретной системы **ОР-3.1** Используя поисковые системы в сети Интернет, умеет находить литературные источники (статьи, книги, руководства пользователей программ), связанные с формальной верификацией программ, анализом корректности программных и аппаратных реализаций алгоритмов защиты информации **ОР-4.1** Умеет применять инструмент fsmtestonline.ru для построения полных проверяющих тестов **ОР-4.1** Умеет применять инструмент SPIN в режиме симуляции и верификации **ПР-1.1** Знает о различных критериях безопасного взаимодействия процессов/программ **ПР-1.2** Умеет проверять свойства распределенных систем, в том числе, свойство безопасности **ПР-2.1** Умеет описывать модели распределенных систем на языке Promela **ПР-2.2** Умеет задавать верифицируемые свойства на языке Promela	*Объяснение материала (лекционные занятия)* *Изучение учебного материала* *Лабораторные работы* *Выполнение проверочной работы* *Работа в электронном курсе* *Работа в МООК*	*Защита лабораторных работ* *Проверочные работы* *Экзамен*

Содержание дисциплины							
Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Раздел 1. Введение в формальные методы верификации	2					2	Изучение учебного материала
Раздел 2. Верификация на основе конечно-автоматной модели	14		16	1,2		20	Изучение учебного материала Подготовка к лабораторным работам Работа в электронном курсе Работа в МООК
Раздел 3. Верификация моделей программ (model checking)	8			1		5	Изучение учебного материала
Раздел 4. Язык Promela и верификатор Spin	8		16	1		13,8	Изучение учебного материала Подготовка к лабораторным работам
Подготовка к промежуточной аттестации в форме экзамена						33,7	Изучение учебного материала
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32		32	5,2	0,3	74,5	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100 %	В сессию	Отлично – сформированные системные знания; успешно применяемые навыки и умения. Хорошо – сформированные, но содержащие отдельные пробелы знания; в целом успешно применяемые навыки и умения. Удовлетворительно – общие, но не структурированные знания; частично освоенные навыки и умения. Неудовлетворительно – отсутствие либо фрагментарность знаний/навыков.

Литература

1. Кудрявцев В. Б. Теория автоматов : Учебник Для бакалавриата и магистратуры / Кудрявцев В. Б., Алешин С. В., Подколзин А. С.. - Москва : Юрайт, 2019. - 320 с.
2. Старолетов С. М. Основы тестирования и верификации программного обеспечения / Старолетов С. М.. - Санкт-Петербург : Лань, 2020. - 344 с.. URL: https://e.lanbook.com/book/138181.
3. Камкин, Александр Сергеевич. Введение в формальные методы верификации программ: учебное пособие /. А. С. Камкин. – Москва: МАКС Пресс, 2018. – 272 с.
4. Шошмина И. В., Карпов Ю. Г. Введение в язык Promela и систему комплексной верификации Spin. Учебное пособие – СПб.: СПбГПУ, 2010. – 111 с.
5. Евтушенко Н.В. Недетерминированные автоматы: анализ и синтез: учебное пособие, ч.1 / Н. В. Евтушенко, А.Ф. Петренко, М. В.Ветрова. Томск: Том. гос. ун-т, 2006. – 142 с.
6. Евтушенко Н.В. Недетерминированные автоматы: анализ и синтез: учебное пособие, ч.3 / Н. В. Евтушенко, М. Л. Громов, Н. В. Шабалдина. Томск: Том. гос. ун-т, 2013. – 57 с.
7. Гилл А. Введение в теорию конечных автоматов / А. Гилл; под ред. П.П. Пархоменко. М. : Наука, Физматлит, 1966, 272 с.

Дополнительные рекомендации к дисциплине

1. Н.В. Шабалдина, С.А. Прокопенко, С.Н. Торгаев, М.Л. Громов, А.В. Лапутенко. Математика в тестировании дискретных систем [Электронный ресурс]. – URL: https://stepik.org/course/73866.
2. Test Generation for Finite State Machine [Электронный ресурс]. – URL: http://www.fsmtestonline.ru/
3. Карпов Ю.Г., Шошмина И.В. Математическая логика [Электронный ресурс].– URL: https://openedu.ru/course/spbstu/MATLOG/.
4. Verifying Multi-threaded Software with SPIN. – URL: http://spinroot.com/

Б1.Б.2.02 Безопасность веб-приложений
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	5 курс 9 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Колегов Денис Николаевич, к.т.н., доцент, доцент кафедры компьютерной безопасности	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Компьютерные сети, Основы построения защищённых компьютерных сетей	

Цель и задачи дисциплины

Цель: формирование у студентов знаний об основных типах атак на веб-приложения и методах их предотвращения.

Задачи:

– изучить основные элементы и механизмы веб-приложений (протокол HTTP, модель DOM, политика SOP, веб-браузеры, веб-серверы, балансировщики нагрузки);

– изучить основные атаки на веб-приложения: XSS, SQL, CSRF, IDOR и др.

– научить обнаруживать и защищаться от атак рассматриваемых классов.

Результаты обучения	Методы обучения	Методы оценивания
Знать: основные виды уязвимостей программного кода; основные методы анализа безопасности веб-приложений; основные методы исследования компьютерных систем с целью выявления уязвимостей веб-приложений. **Уметь**: проводить анализ безопасности веб-приложений; проводить работы по оценке защищенности веб-приложений и составлять отчёты по результатам проведённых работ; разрабатывать и применять инструментальные средства выявления уязвимостей веб-приложений. **Владеть**: инструментальными средствами анализа защищенности и выявления уязвимостей веб-приложений; Навыками выявления и документирования уязвимостей веб-приложений.	• Лекции • Самостоятельная работа	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Архитектура веб-приложений.	2					2	Изучение учебного материала.
Поиск уязвимостей к атакам CSRF.	4					4	Изучение учебного материала.
Поиск уязвимостей к атакам XSS.	6					6	Изучение учебного материала.
Поиск уязвимостей к атакам SQLI.	6					6	Изучение учебного материала.
Поиск уязвимостей к атакам IDOR.	4					4	Изучение учебного материала.
Поиск уязвимостей в механизмах управления сессиями.	6					6	Изучение учебного материала.

Методы автоматизации поиска уязвимостей.	4					4	Изучение учебного материала.
Подготовка к зачету				1,6		6,15	
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
- Зачет	100 %	В конце семестра	**Зачтено**: студент владеет большей частью теоретического материала **Незачтено**: студент не освоил большую часть теоретического материала.

Литература

1. Л. Шкляр, Р. Розен. Архитектура веб-приложений. - М.: Эксмо, 2011. - 640 с.
2. OWASP Testing Guide. URL: https://www.owasp.org/index.php/OWASP Testing Guide v4 Table of Contents.

Дополнительные рекомендации к дисциплине

Перечень ресурсов информационно-телекоммуникационной сети Интернет:

1. Страница курса на Github.com: https://github.com/tsu-iscd/web-application-security/blob/master/README.md.
2. В. Кочетков. Как разработать защищенное веб-приложение и не сойти при этом с ума? -URL: http://my.webinar.ru/record/140584/.
3. В. Кочетков. Философия Application Security. URL: https://www.youtube.com/watch?v=mb7tcT-9VXk
4. В. Кочетков. Прикладная теория безопасности приложений. – URL: https://my.webinar.ru/record/622509/?i=574d3d07f32978bOae039c8604b45409

Перечень информационных технологий, используемых при осуществлении образовательного процесса: Burp Suite, OWASP ZAP, VirrualBox или VMWare Player, Kali Linux.

Б1.Б.2.03 Алгоритмы кодирования и сжатия информации
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	2 курс 4 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Жабин Иван Владимирович, ассистент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Дискретная математика, Языки программирования	Алгоритмы и структуры данных I, II

Цель и задачи дисциплины

Цель: изучить основные понятия теории кодирования и сжатия и научиться самостоятельно строить алгоритмы кодирования и сжатия.

Задачи:

- изучить основные понятия теории кодирования (код, префиксность, разделимость, сильная разделимость, полнота, избыточность, оптимальность кода);
- рассмотреть алгоритмы кодирования (код Фано, код Шеннона, код Хаффмана);
- изучить различные алгоритмы сжатия информации, такие как арифметическое сжатие, метод линейного предсказания, словарные алгоритмы сжатия, контекстное моделирование, преобразование Барроуза — Уиллера и сопутствующие алгоритмы сжатия и др.
- изучить алгоритмы сжатия звука изображений и видео

Результаты обучения	Методы обучения	Методы оценивания
Знать: проблемы кодирования и сжатия информации; основные понятия теории кодирования и сжатия информации; основные теоремы, описывающие свойства кодов и алгоритмов кодирования и сжатия информации; основные свойства кодов и алгоритмов шифрования и сжатия информации; современные тенденции развития основных алгоритмов кодирования и сжатия различных видов информации; основные вычислительные алгоритмы, реализующие современные методы кодирования и сжатия информации. **Уметь**: применять теоремы и основные свойства кодов и алгоритмов кодирования и сжатия информации для построения основных алгоритмов кодирования и сжатия информации; учитывать тенденции развития основных алгоритмов кодирования и сжатия различных видов информации; реализовать современные вычислительные алгоритмы, реализующие современные методы кодирования и сжатия информации. **Владеть**: навыками самостоятельного построения основных алгоритмов кодирования и сжатия информации; современными тенденциями развития алгоритмов кодирования и сжатия различных видов информации; современными вычислительными алгоритмами, реализующими современные методы кодирования и сжатия информации.	• Лекции • Лабораторные работы • Самостоятельна работа	Зачет с оценкой

Содержание дисциплины							
Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет с оценкой	Часы СРС	Задания
Основные задачи кодирования	2					2	Изучение учебного материала.
Разделимые и сильно разделимые коды	2					2	Изучение учебного материала.
Автоматность и сильная разделимость	2					2	Изучение учебного материала.
Код Фано, код Шеннона. Оценки	2		8			4	Изучение учебного материала. Подготовка к лабораторным занятиям
Оптимальные коды. Код Хаффмана	2		8			4	Изучение учебного материала. Подготовка к лабораторным занятиям
Арифметическое сжатие	2		16			6	Изучение учебного материала. Подготовка к лабораторным занятиям
Нумерующее кодирование. Векторное квантование	2					2	Изучение учебного материала.
Метод линейного предсказания. Субполосное кодирование	2					2	Изучение учебного материала.
Словарные алгоритмы сжатия	2					2	Изучение учебного материала.
Методы контекстного моделирования	2					2	Изучение учебного материала.
Преобразование Барроуза — Уоллера и сопутствующие алгоритмы сжатия	2					2	Изучение учебного материала.
Сжатие изображений без потерь	2					2	Изучение учебного материала.
Сжатие видеоданных	2					2	Изучение учебного материала.
Сжатие звуковых данных	2					2	Изучение учебного материала.
Алгоритмы фрактального сжатия изображений	2					2	Изучение учебного материала.
Вейвлеты	2					2	Изучение учебного материала.
Подготовка к промежуточной аттестации в форме зачета с оценкой				1,6		2,15	
Прохождение промежуточной аттестации в форме зачета с оценкой					0,25		
Всего	32		32	1,6	0,25	42,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет с оценкой	100%	В конце семестра	**Отлично**: знание и понимание материала в полном объеме. **Хорошо**: хорошее знание материала за исключением

			некоторых деталей. **Удовлетворительно:** не глубокое понимание материала, на уровне общих представлений. **Неудовлетворительно**: незнание и непонимание материала даже на уровне общих представлений

Литература

Основная литература:

1. Яблонский С.В. Введение в дискретную математику. – М.: Высшая школа, 2010. – 381с.
2. Сэломон Д. Сжатие данных изображений и звука. – М.: Техносфера, 2010. – 381 с.

Дополнительная:

1. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: Диалог-МИФИ, 2002. – 384с.
2. Уэлстид С. Фракталы и вейвлеты для сжатия изображений в действии – М.: Триумф, 2003. —320 с.
3. Дискретная математика и математические вопросы кибернетики / Под ред. С.В. Яблонского и О.Б, Лупанова, М.: Наука, 1974. —312 с.

Дополнительные рекомендации к дисциплине

Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. http://mathtree.ru
2. http://mathnet.ru
3. http://arxiv.jrgmathnet.ru

Б1.Б.2.04 Теория кодирования, сжатия и восстановления информации
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	4 курс 8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Пахомова Елена Григорьевна, к.ф.-м.н, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Алгебра; Комбинаторика; Криптографические методы защиты информации; Алгоритмы кодирования и сжатия информации	Основы построения защищённых баз данных; Основы построения защищённых компьютерных сетей

Цель и задачи дисциплины

Цель:

- дать студентам представление о помехоустойчивом кодировании и его практическом применении

Задачи:

- изучить основы теории кодирования
- изучить базовые помехоустойчивые коды

Результаты обучения	Методы обучения	Методы оценивания
Обучающийся должен: • **знать:** базовую терминологию, основные методы кодирования и декодирования; основные границы на объём кода; основные применения кодов в криптографии; • **уметь:** применять теорию кодирования при решении задач защиты информации; • **владеть:** базовыми алгоритмами теории кодирования; • обладать следующими компетенциями, перечисленными в ООП: ОПК-2, ПСК-1,5.	• Лекции • Практические занятия	• Экзамены в 8 семестре • Уровень выполнения самостоятельных работ

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Введение в предмет теории кодирования. Коды минимальной избыточности	4	2				2,7	Изучение теоретического материала. Выполнение практических заданий
Границы для кода	4					1,8	Изучение теоретического материала.
Линейный код	4	2				2,7	Изучение теоретического материала. Выполнение практических заданий
Коды Хэмминга	2	2				1,8	Изучение теоретического материала. Выполнение практических заданий
Линейный МДР-код	2					0,9	Изучение теоретического материала.
Коды Рида-Маллера. Мажоритарное декодирование	4	2				2,7	Изучение теоретического материала. Выполнение практических заданий
Обобщённый код Рида-Соломона	2	2				1,8	Изучение теоретического материала. Выполнение практических заданий
Коды Голея	2	2				1,8	Изучение теоретического материала.

							Выполнение практических заданий
Циклический код. БЧХ-код	8	4				5,4	Изучение теоретического материала. Выполнение практических заданий
Подготовка к прохождению промежуточной аттестации в форме экзамена				2,4		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	16		4,4	0,3	55,3	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
- Самостоятельные работы 1-6	Самостоятельные работы – 20%	В течение семестра	**Отлично**: знание и понимание материала в полном объеме. **Хорошо**: хорошее знание материала за исключением некоторых деталей. **Удовлетворительно:** не глубокое понимание материала, на уровне общих представлений.
- Экзамен	Экзамен – 80%	В конце семестра	

Литература

- **Основная литература:**

1. Штарьков Ю. М. Универсальное кодирование : теория и алгоритмы / Ю. М. Штарьков; Ин-т проблем передачи информации им. А. А. Харкевича Рос. акад. наук. - Москва : Физматлит, 2013. - 279 с.: ил.
2. Шень А., Румянцев А., Ромащенко А., Заметки по теории кодирования. МЦНМО. 2011. 80 с.
3. Сагалович Ю.Л. Введение в алгебраические коды. М.: ИППИ РАН. 2010. 302 с.
4. Сидельников В. Теория кодирования. ФИЗМАТЛИТ. 2008. 324 с.

- **Дополнительная литература**

5. Чечета С. Введение в дискретную теорию информации и кодирования. МЦНМО. 2011. 224 с.
6. Колесник В.Д. Кодирование при передаче и хранении информации (алгебраическая теория блоковых кодов). М.: Высш. Школа. 2009. 550 с.
7. Кудряшов Б.Д. Теория информации. СПб.: Питер. 2009. 213 с.
8. Евтушенко Н. В. Коды, исправляющие ошибки : учебно-методический комплекс / Евтушенко Н. В., Коломеец А. В., Попов Д. Д. ; Том. гос. ун-т, Ин-т дистанционного образования. - Томск : ИДО ТГУ, 2007. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000244211
9. Дайняк А. Б. Конспект лекций по теории кодирования [Электронный ресурс] / Дайняк А. Б. Некоторые вопросы теории кодов, исправляющих ошибки : учебно-методическое пособие — М.: МФТИ, 2013. — 44 с. URL: http://www.dainiak.com/ru/teaching/books

Дополнительные рекомендации к дисциплине

Базы данных и информационно-справочные системы, в том числе зарубежные

1. Волков А. Теория помехоустойчивого кодирования [Электронный ресурс] / Видеолекции НГУ: Теория Помехоустойчивого Кодирования, 2006 – 2016. URL: https://www.youtube.com/playlist?list=PLHKx-rx3MlyE5vjrd4bv91LAGs9_AdBCu
2. Ромащенко А. Теория кодирования // Просветительский проект «Лекториум» – 2019. - URL: https://www.lektorium.tv/course/22864 (дата обращения: 01.09.2019)
3. Скачек В. Классическая теория кодирования и новые приложения // Просветительский проект «Лекториум» – 2019. – https://www.lektorium.tv/node/36857 (дата обращения: 01.09.2019)
4. Еханин Сергей. Локальное декодирование // Просветительский проект «Лекториум» – 2019. – https://www.lektorium.tv/course/22879 (дата обращения: 01.09.2019)
5. Шень Александр. Ликбез: коды, исправляющие ошибки // Просветительский проект «Лекториум» – 2019. – https://www.lektorium.tv/node/31751 (дата обращения: 01.09.2019)

Б1.Б.2.05 Анализ уязвимостей программного обеспечения
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	5 курс семестр А	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Брославский Олег Викторович, ассистент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
• Языки программирования; • Операционные системы;	

Цель и задачи дисциплины

Цель: изучение студентом основных видов уязвимостей программного обеспечения; освоение основных методов и средств анализа и устранения уязвимостей программных реализаций.

Задачи:

- формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;
- формирование навыков анализа программных реализаций на предмет наличия уязвимостей.

Результаты обучения	Методы обучения	Методы оценивания
Знать: • способы, методы и критерии оценки эффективности реализации систем защиты информации; • основные средства и методы анализа программных реализаций на предмет уязвимостей; • статические и динамические методы анализы программных реализаций. Уметь: • выявлять и устранять уязвимости программных реализаций и локализовать их последствия; • проводить экспертизу качества и надежности программных и программно-аппаратных средств обеспечения информационной безопасности. Владеть: • приёмами анализа программных реализаций на предмет наличия уязвимостей.	• Лекции • Практические занятия • Лабораторные работы	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Тема 1. Понятие и классификация уязвимостей программного обеспечения		2					Изучение учебного материала.
Тема 2. Актуальные уязвимости		3	8			4	Изучение учебного материала.

современного программного обеспечения							Выполнение лабораторных работ
Тема 3. Уязвимости этапа проектирования программного обеспечения		3	8			4	Изучение учебного материала. Выполнение лабораторных работ
Тема 4. Предотвращение уязвимостей на этапе реализации		3	8			4	Изучение учебного материала. Выполнение лабораторных работ
Тема 5. Анализ бинарных уязвимостей программного обеспечения		5	24			24	Изучение учебного материала. Выполнение лабораторных работ
				3,45		4,55	Подготовка к сдаче зачета
Всего		16	48	3,45		40,55	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Лабораторные работы	50	В течение семестра	Корректность выполнения лабораторной работы. Понимание использованных подходов и технологий.
Зачет	50	В конце семестра	Полнота ответа на вопросы экзаменатора

Литература

- Linux глазами хакера. - 6-е изд. М. Е. Фленов, 2021.
- Penetration Testing: A Hands-On Introduction to Hacking. Georgia Weidman. 2014.

Дополнительные рекомендации к дисциплине

- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Dafydd Stuttard, Marcus Pinto. Wiley; 2nd edition (September 27, 2011)
- Hacking: The Art of Exploitation, 2nd Edition. Jon Erickson. No Starch Press; 2nd edition (February 4, 2008)

Б1.В.01 Элективные дисциплины по физической культуре и спорту
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
328	Специалитет	1 курс / 1-2 семестр, 2 курс / 3-4 семестр, 3 курс / 5-6 / 6 семестров	обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Иноземцева Татьяна Андреевна, старший преподаватель	Факультет физической культуры, кафедра физической культуры и спорта

Пререквизиты	Параллельно осваиваемые дисциплины
Базовый курс общеобразовательных знаний	Физическая культура и спорт

Цель и задачи дисциплины

Цель дисциплины - формирование физической культуры личности студента и способности реализовать ее в социально-профессиональной, физкультурно-спортивной и оздоровительной деятельности.
Задачи дисциплины: всестороннее развитие и совершенствование личности, формирование отношений к здоровому образу жизни.

Результаты обучения	Методы обучения	Методы оценивания
Понимает роль физической культуры и спорта в современном обществе, в жизни человека, подготовке его к социальной и профессиональной деятельности, значение физкультурно-спортивной активности в структуре здорового образа жизни и особенности планирования оптимального двигательного режима с учетом условий будущей профессиональной деятельности. Использует методику самоконтроля для определения уровня здоровья и физической подготовленности в соответствии с нормативными требованиями и условиями будущей профессиональной деятельности. Составляет комплекс упражнений в соответствии с группой здоровья, комплексы профессионально-прикладной физической культуры с учетом особенностей будущей профессиональной деятельности.	• Практики	Зачет

Содержание дисциплины

Темы занятий	Контактные часы				Самостоятельная работа	
	Лекции	Практики	Лабораторные занятия	Консультации	Часы СРС	Задания
Всего:	0	328	0	0	0	

Литература

Письменский И. А., Аллянов Ю. Н. Физическая культура: учебник для академического бакалавриата. – Москва: Юрайт, 2016.
Барчуков И. С. Физическая культура: методики практического обучения. – Москва: Кнорус, 2014.

Б1.В.02 Теория чисел
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
4 з.е.	Специалитет	3-й курс, 5 семестр	Вариативная часть, обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Чехлов Андрей Ростиславович, доктор физико-математических наук	Механико-математический факультет

Пререквизиты	Параллельно осваиваемые дисциплины
Знания: - базовых курсов математического анализа ВУЗа и алгебры университета; - основ теории множеств, дискретной математики; - основ теории кодирования, математической логики и теории алгоритмов. **Умения:** - определять стандартные задачи теории чисел и подбирать методы их решения; - обосновывать ход решения задач теоретическими фактами; - доказывать основные теоремы теории чисел.	«Системы управления базами данных», «Языки программирования», «Технология разработки программ»

Цель и задачи дисциплины

Цель дисциплины: овладение студентами математическим аппаратом теории чисел, фундаментальными теоретическими и прикладными положениями этой науки.

Задачи дисциплины: формирование системы знаний и умений в области теории чисел; воспитание математической культуры, необходимой будущему математику для понимания целей и задач своей профессиональной деятельности; обеспечение понятийной базы для других предметов, использующих теорию чисел в качестве поставщика понятий и необходимого математического аппарата (теория алгоритмов, дискретная математика, информатика, компьютерная алгебра, и др.).

Результаты обучения	Методы обучения	Методы оценивания
- освоение методологии построения математических моделей; - пополнение запаса стандартных алгоритмов для решения задач теоретико-числовыми методами; - получение представлений о современных тенденциях развития теории чисел.	• Лекции • Практические занятия • Индивидуальная самостоятельная работа	• Индивидуальные задания • Тесты • Экзамен

Содержание дисциплины

Темы занятий	Контактные часы				Самостоятельная работа	
	Лекции	Практические занятия	Консультации	Экзамен	Часы СРС	Задания
1. Делимость и простые числа. Теорема о делении с остатком. НОД чисел. Алгоритм Евклида. Простые числа. Основная теорема	4	4			4	

арифметики.						
2. Арифметические функции. Мультипликативные функции и их примеры.	5	5			4	
3. Цепные дроби.	4	4			4	
4. Сравнения 1-й степени	4	4			5	
5. Индивидуальное задание					4	Задание в системе Moodle.
6. Сравнения n-степени.	5	5			6	
7. Сравнения 2-степени	4	4			6	
8. Первообразные корни и индексы.	6	6			5	
9. Тесты					2,8	Тесты в системе Moodle.
Подготовка к прохождению промежуточной аттестации в форме экзамена			3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена			2	0,3		
Всего	32	32	5,2	0,3	74,5	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Инд. задание в системе Moodle.	20%	В течение семестра	По 100 бальной системе.
Тесты в системе Moodle.	30%	В течение семестра	Максимальное использование возможностей программы
Экзамен	50%	В конце семестра	Студент допускается до экзамена только при наличии выполненных индивидуального задания и теста. 1) Полный ответ, изложенный кратко и ясно – «отлично». 2) Ответ неполный (но > 80%), пояснения логически непротиворечивы – «хорошо». 3) Ответ неполный (но > 50%), есть запинки в логике и пояснениях – «удовлетворительно». 4) Ответ неполный (< 50%), отсутствие логики в пояснениях – «неудовлетворительно».

Обязательная литература

1. Кузьмина А. С., Мальцев Ю. Н. Теория чисел. Барнаул, 2011. 240 с.
2. Бухштаб А. А. Теория чисел. Лань. 2015. 384 с.
3. Виноградов, И.М. Основы теории чисел. 2003. 176 с.

Рекомендуемая литература

1. Деза Е. И., Котова Л. В. Сборник задач по теории чисел. М.: Либроком/URSS, 2012. 224 с.
2. Манин Ю. И., Панчишкин А.А. Введение в современную теорию чисел. М.: МЦНМО, 2013. 552 с.
3. Сушкевич А.К. Теория чисел. М.: Вузовская книга, 2016. 240 с.
4. Арнольд И.В. Теория чисел. М.: Ленанд, 2019. – 288 с.
5. Боревич З.И., Шафаревич И.Р. Теория чисел. М.: Ленанд, 2019. – 504 с.
6. Куликов Л. Я., Москаленко А. И., Фомин А. А. Сборник задач по алгебре и теории чисел. М.: Просвещение, 1993. 288 с.

Дополнительные рекомендации к дисциплине

Основная информация по технологиям, изучаемым в курсе, содержится на сайтах:
1) http://alexhvorost.narod2.ru/
2) https://www.youtube.com/playlist?list=PL2ar10WmyGU5A6qkfwbujIMJYXR6S5PiP
3) https://ru.wikipedia.org/wiki/Теория_чисел
Курс в MOODLE ТГУ:
http://class.tsu.ru/m-course-12935

Б1.В.03 Введение в математику
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	1 курс 1 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Панкратова Ирина Анатольевна, к.ф.м.н., доцент	Лаборатория компьютерной криптографии

Пререквизиты	Параллельно осваиваемые дисциплины
	Дискретная математика (булевы функции)

Цель и задачи дисциплины

Цель: изложение тех начальных элементов математического языка, теории множеств, математической логики и абстрактной алгебры, которые позволят студенту успешно овладеть современной математикой, лежащей в основе всех дисциплин математического и естественнонаучного, профессионального и специального циклов ООП по специальности Компьютерная безопасность.

Задачи: обучить студентов математическому языку и методам логических рассуждений и доказательств, используемым при теоретико-множественном изложении математики.

Результаты обучения	Методы обучения	Методы оценивания
Знать понятия переменной, константы, множества, кортежа (вектора), соответствия, отношения, отображения, функции, операции; основные операции над высказываниями, высказывательными формами, предикатами, множествами, отношениями **Уметь** выражать содержательные высказывания в математической форме; доказывать утверждения на математическом языке путём логических рассуждений **Владеть** в совершенстве начальными понятиями математики	• Лекции • Практики	Зачет с оценкой

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет с оценкой	Часы СРС	Задания
Основные понятия теории множеств	6	6				2	Изучение учебного материала. Решение задач Подготовка к контрольным
Определения и доказательства по индукции	2	2				2	
Формулы алгебры высказываний	4	4				2	
Формулы алгебры предикатов	4	4				2	
Кортежи	2	2				2	
Разбиение множества	2	2				2	
Отношения; свойства и операции над бинарными отношениями	4	4				2,8	
Отношение эквивалентности	2	2				2	
Отношение частичного порядка	2	2				2	
Отображения	2	2				2	
Подстановки	2	2				2	
Подготовка к промежуточной аттестации в форме зачёта с оценкой						15,75	
Прохождение промежуточной				2	0,25		

аттестации в форме зачета с оценкой							
Всего	32	32		5,2	0,25	38,55	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Вид оцениваемой работы:			
Контрольные работы	40	В течение семестра	Владение основными понятиями Умение решать задачи
Зачет с оценкой	60	В конце	Владение теорией

Литература

- *Агибалов Г.П., Панкратова И.А.* Введение в математику – Томск: ТГУ, 2022.
- *Rasiowa H.* Introduction to modern mathematics. Amsterdam: PWN jointly with North-Holland-Publishing Company, 1973.
- *Шиханович Ю.А.* Введение в современную математику. М.: Наука, 1965.
- *Успенский В.А.* Апология математики. СПб.: Амфора, 2011.
- *Лавров И.А.*, *Максимова Л.Л.* Задачи по теории множеств, математической логике и теории алгоритмов. М.: Наука, 1975.

Б1.В.04 Комбинаторика
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	4 курс 7 семестр	Входит в вариативную часть, обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Останин Сергей Александрович, к.т.н., доцент	кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Введение в математику, Дискретная математика, Алгебра, Математический анализ	Криптографические методы защиты информации

Цель и задачи дисциплины

Цель: курс посвящён перечислительной комбинаторике. Её основная задача состоит в перечислении (подсчёте и генерации) объектов, удовлетворяющих определённым ограничениям. Комбинаторика связана со всеми основными разделами современной математики: с анализом, топологией, алгеброй и геометрией, с дискретной математикой. Её результаты используются в теории кодирования и криптографии.
Задачи: рассмотреть следующие темы: основные комбинаторные объекты и принципы, основные комбинаторные числа и тождества для них, комбинаторные теоремы теории графов, комбинаторика частично упорядоченных множеств, принцип включений и исключений, обращение Мёбиуса, комбинаторные схемы, системы Штейнера, аффинные и проективные плоскости и геометрии, производящие функции, разбиения.

Результаты обучения	Методы обучения	Методы оценивания
Знать: основные комбинаторные принципы, основные комбинаторные числа и тождества для них, принцип включений и исключений, принцип обращения Мёбиуса, понятие производящей функции **Уметь**: решать типовые перечислительные задачи, используя основные комбинаторные принципы **Владеть**: основными методами решения перечислительных задач комбинаторики	• Лекции • Практические занятия • Самостоятельная работа	• Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Основные комбинаторные объекты н принципы	4	4				2	Изучение учебного материала. Подготовка к практическим занятиям
Комбинаторные числа н тождества	4	4				2	Изучение учебного материала. Подготовка к практическим занятиям
Факториал Бхаргавы	2	2				2	Изучение учебного материала. Подготовка к практическим занятиям
Комбинаторные теоремы теории графов	4	4				2	Изучение учебного материала. Подготовка к практическим занятиям
Антицепи в булевом кубе	4	4				4	Изучение учебного материала. Подготовка к практическим занятиям
Принцип включений и исключений, принцип обращения Мёбиуса	4	4				2	Изучение учебного материала. Подготовка к практическим занятиям
Комбинаторные схемы, системы	4	4				4	Изучение учебного материала.

Штейнера. Проективные и аффинные плоскости							Подготовка к практическим занятиям
Производящие функции	4	4				2	Изучение учебного материала. Подготовка к практическим занятиям
Теневое исчисление	2	2				2,8	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к сдаче экзамена				3,2		15,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	32		5,2	0,3	38,5	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100 %	В конце семестра	Должны быть сданы обязательные практические задания, иначе оценка "Неудовлетворительно". **Отлично**: студент полностью владеет теоретическим материалом; **Хорошо**: студент полностью владеет теоретическим материалом, но допускает ошибки или неточности; **Удовлетворительно**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает ошибки; **Неудовлетворительно**: студент не сдал обязательные практические задания и/или не освоил большую часть теоретического материала.

Литература

Основная литература
1. Рональд Л. Грэхем, Дональд Эрвин Кнут, Орен Поташник. Конкретная математика. Математические основы информатики. Вильямс. 2015. – 784 с.
2. Виленкин Н., Виленкин А., Виленкин П. Комбинаторика, 2015. – 400 с.
Дополнительная литература
1. Холл М. Комбинаторика. М.: МИР, 1970. – 421 с.
2. Риордан Дж. Введение в комбинаторный анализ. ИЛ. 1963. – 287 с.
3. Стенли Р. Перечислительная комбинаторика. Деревья, производящие функции и симметрические функции. 2005, – 768 с.
4. Сачков В.Н. Введение в комбинаторные методы дискретной математики. – М.: Изд-во МЦНМО, 2004.

Дополнительные рекомендации к дисциплине

1. http://mathtree.ru
2. http://mathnet.ru
3. https://aixiv.org/archive/math

Б1.В.05 Булевы функции в криптографии
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	4 курс 8 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Панкратова Ирина Анатольевна, к.ф.м.н., доцент	Лаборатория компьютерной криптографии

Пререквизиты	Параллельно осваиваемые дисциплины
Введение в математику Дискретная математика Языки программирования Методы программирования	

Цель и задачи дисциплины

Цель: изучение криптографических свойств булевых функций

Задачи: изучить теоретические основы и практические алгоритмы вычисления криптографических характеристик булевых функций

Результаты обучения	Методы обучения	Методы оценивания
Формирование у студентов профессиональных компетенций в соответствии с ФГОС ВО по специальности Компьютерная безопасность путём привития им знаний криптографических свойств булевых функций, навыков в методах оценивания криптографических свойств булевых функций и умения применять их в профессиональной деятельности.	• Лекции • Лабораторные работы	Зачет с оценкой

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Корреляционная иммунность	8		10	1		10	Изучение учебного материала. Подготовка к лабораторным занятиям
Нелинейность	10		8	1		10	
Лавинные характеристики	6		6	0,5		8	
Алгебраическая иммунность	4		6	0,5		8	
Запреты булевых функций	4		2	0,45		4,55	
Всего	32		32	3,45		40,55	

Оценивание

Вид работы	Удельный вес	Период	Критерии оценки
Вид оцениваемой работы: Программа Контрольная работа Зачет с оценкой	 50 10 40	 В течение семестра В конце	Критерии оценивания указанного вида работы Качество программ Владение алгоритмами Владение теорией

Литература

1. *Агибалов Г.П.* Избранные теоремы начального курса криптографии. – Томск: НТЛ, 2005.
2. *Бабаш А.В.*, *Шанкин Г.П.* Криптография. М.: СОЛОН-Р, 2002.
3. *Лобанов М.С.* Точное соотношение между нелинейностью и алгебраической иммунностью // Дискретная математика. 2006. Т.18. Вып.3. С.152-159.
4. *Логачев О.А.*, *Сальников А.А.*, *Ященко В.В.* Булевы функции в теории кодирования и криптологии. – М: МНЦМО, 2004.
5. *Панкратова И.А.* Булевы функции в криптографии: учебное пособие. Томск: Изд. Дом ТГУ, 2014; СПб: Лань, 2019.
6. *Таранников Ю.В.* О корреляционно-иммунных и устойчивых булевых функциях // Мат. вопросы кибернетики. Вып.11. 2002. С.91-148.
7. *Токарева Н.Н.* Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. № 1. С.15-37.
8. *Токарева Н.Н.* Обобщения бент-функций. Обзор работ // Дискрет. анализ и исслед. операций. 2010. Т.17. № 1. С.34-64.
9. *Уоррен Г.* Алгоритмические трюки для программистов. М.: Вильямс, 2003.
10. *Фомичёв В.М.* Дискретная математика и криптология. М.: Диалог-МИФИ, 2003.
11. *Courtois N.*, *Meier W.* Algebraic attack on stream ciphers with linear feedback // LNCS. 2003. V.2656. P.345-359.
12. *Dalai D.K.* On some necessary conditions of Boolean functions to resist algebraic attack. Ph. D. Thesis. Kolkata, India, 2006.
13. *Meier W., Pasalic E., Carlet C.* Algebraic attack and decomposition of Boolean functions // LNCS. 2004. V.3027. P.474-491.

Б1.В.06 Профессиональный перевод специальной литературы
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
7 з.е.	специалитет	3 курс 5, 6 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Бутузова Татьяна Владимировна, ст. преподаватель	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Необходимы компетенции, сформированные в результате освоения дисциплин на первом и втором курсе	

Цель и задачи дисциплины

Цель сформировать умение использовать материалы современных исследований в профессиональной области на иностранном языке; обучить работать со специальной литературой с целью получения профессиональной информации; привить основные навыки обработки информации, полученной из специальной литературы.

Результаты обучения	Методы обучения	Методы оценивания
Знать: – лексический и грамматический минимум в объеме, необходимом для работы с текстами профессиональной направленности и осуществления коммуникации на иностранном языке; **Уметь**: – читать и переводить научно-техническую литературу на иностранном языке по профессиональной тематике, правильно употреблять терминологическую лексику в профессиональной речи; **Владеть**: – иностранным языком в объеме, необходимом для получения и изложения информации по профессиональной тематике, навыками общения на иностранном языке;	• Практические занятия • Самостоятельная работа	• Зачет • Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен/Зачет	Часы СРС	Задания
5 семестр Теория и практика перевода Научный стиль							
Особенности научного стиля Грамматика: порядок слов в английском предложении		6				4	Изучение учебного материала. Подготовка к практическим занятиям
Знакомство с базовыми понятиями. Создание тематического глоссария. Грамматика: глагол, видовременные формы глагола.		6				4	Изучение учебного материала. Подготовка к практическим занятиям
Знакомство со структурой научной статьи. Грамматика: сложности перевода глагола в страдательном залоге.		8				4	Изучение учебного материала. Подготовка к практическим занятиям
Abstract (особенности написания) Грамматика: существительное;		6				4	Изучение учебного материала. Подготовка к практическим занятиям

существительное в роли определения (правило атрибутивного ряда)							
Introduction (анализ содержания). Грамматика: множественное число существительного.		6				4	Изучение учебного материала. Подготовка к практическим занятиям
Предпереводческий анализ и перевод текста /Чтение и анализ научно-технических статей.		2					
Ссылки на источники правило оформления). Грамматика: слова-заменители существительного		6				4	Изучение учебного материала. Подготовка к практическим занятиям
Conclusion (анализ содержания). Грамматика: неопределенная форма глагола. Обороты с неопределенной формой глагола.		6				4	Изучение учебного материала. Подготовка к практическим занятиям
Грамматика: герундий; обороты с герундием.		8				4	Изучение учебного материала. Подготовка к практическим занятиям
Грамматика: причастие; обороты с причастием.		8				4	Изучение учебного материала. Подготовка к практическим занятиям
Предпереводческий анализ и перевод текста /Чтение и анализ научно-технических статей.		2					
Подготовка к сдаче зачета				3,2		4,55	
Прохождение промежуточной аттестации в форме зачета					0,25		
Итого		64		3,2	0,25	40,55	
6 семестр Теория и практика перевода Научный стиль							
Средства логической связи. Грамматика: оборот There (be)		6				6	Изучение учебного материала. Подготовка к практическим занятиям
Презентация: Title. Introduction. Грамматика: виды придаточных предложений.		8				6	Изучение учебного материала. Подготовка к практическим занятиям
Грамматика: придаточные предложения условия		10				6	Изучение учебного материала. Подготовка к практическим занятиям
Презентация: Methods. Materials Грамматика: инверсия. Эллиптические конструкции.		10				6	Изучение учебного материала. Подготовка к практическим занятиям
Предпереводческий анализ и перевод текста /Чтение и анализ научно-технических статей.		2					
Презентация: Results Грамматика: модальные глаголы. Структуры: might+well+ Infinitive Might+Infmitive+well		8				4	Изучение учебного материала. Подготовка к практическим занятиям
Презентация: Conclusion Ложные друзья переводчика		8				4	Изучение учебного материала. Подготовка к практическим занятиям
Деловой английский. Написание CV/Resume. Cover letter		8				4	Изучение учебного материала. Подготовка к практическим занятиям
Перевод аббревиатур		4				4,8	Изучение учебного материала. Подготовка к практическим занятиям
Подготовка к прохождению экзамена				3,2		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Итого		64		5,2	0,3	74,5	
Всего		128		8,4	0,55	115,05	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет (5 семестр)	100 %	В конце семестра	**Зачтено**: студент полностью владеет теоретическим материалом; **Не зачтено**: не освоил большую часть теоретического материала.
Экзамен (6 семестр)	100 %		**Отлично**: студент полностью владеет теоретическим материалом; **Хорошо**: студент полностью владеет теоретическим материалом, но допускает ошибки или неточности; **Удовлетворительно**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает негрубые ошибки; **Неудовлетворительно**: студент не сдал все обязательные практические работы и/или не освоил большую часть теоретического материала.

Литература

Основная литература:

1. Английский язык. Теория и практика перевода. А.А. Тихонов.Москва.Проспект.2005. - 120с.
2. Лексические особенности англо-русского научно-технического перевода. Теория и практика перевода: уч. пособие, Л.И Борисова
3. Английский язык для магистров и аспирантов естественных факультетов университетов. О.И. Сафроненко. Москва. Высшая школа. 2005-175с.
4. Практический курс грамматики английского языка/Т.Н.Михельсон, Н.В. Успенская, Москва: Альянс, 2009. –254 с.
5. Wallwork A. English for Academic Research. SpringerScience, 2013.
6. Information security : principles and practice /Mark StampStamp, Mark. Hoboken : Wiley-Interscience, 2006

Дополнительная литература:

l. CryptoGraphics Электронный ресурс : Exploiting Graphics Cards for Security / /by Debra L. Cook, Angelos D. Keromytis.Cook, Debra L. Boston, MA :: Springer Science+Business Media, LLC, 2006.
2. Computer Viruses and Malware Электронный ресурс /by John Aycock.Aycock, John. Boston, MA :: Springer Science+Business Media, LLC, 2006.
3. Confidentiality and Integrity in Crowdsourcing Systems electronic resource /by Amin Ranj Bar, Muthucumaru Maheswaran.Ranj Bar, Amin. Cham : : Springer International Publishing : : Imprint: Springer, ,2014. V, 77 p. 8
4. Security and Privacy Protection in Information Processing Systems [electronic resource] :: 28th IFIP TC 11 International Conference, SEC 2013, Auckland, New Zealand, July 8-10, 2013. Proceedings / edited by Lech J. Janczewski, Henry B. Wolfe, Sujeet Shenoi.Janczewski, Lech J. Springer Berlin Heidelberg : : Imprint: Springer, 2013.

Дополнительные рекомендации к дисциплине

http://www.loc.gov/catdir/toc/ecip058/2005005152.html
http://www.loc.gov/catdir/eiiliancements/fy0645/2005005152-d.html
http://www.loc.gov/catdii7enhancements/fy0645/2005005152-b.html
http://ck.doi.org/10.1007/0-387-34189-7
http://dx.doi.org/10.1007/0-387-34188-9
http://dx.doi.org/10.1007/978-3-319-02717-3
http://dx.doi.org/10.1007/978-3-642-39218-4

Б1.В.07 Методы компиляции
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	4 курс 8 семестр	Вариативная часть, обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Буторина Наталья Борисовна, старший преподаватель	Кафедра компьютерной безопасности, ИПМКН

Пререквизиты	Параллельно осваиваемые дисциплины
Информатика, Языки программирования.	

Цель и задачи дисциплины

В курсе рассматриваются вопросы разработки трансляторов с языков высокого уровня. Наибольшее внимание в курсе уделяется методам трансляции, основанных на теории формальных грамматик. Дается определение порождающих грамматик и языков, стратегий синтаксического анализа. В курсе рассматривается процесс разработки лексического и синтаксического этапов транслятора на основе данной теории. Наиболее сложным и трудоемким является этап синтаксического анализа. В курсе рассматриваются методы детерминированного анализа восходящей и нисходящей стратегий, позволяющих выполнить грамматический разбор программы без тупиков и возвратов. Выполняется сравнение эффективности методов. В курсе также рассматриваются вопросы и методы оптимизации программ.

Результаты обучения	Методы обучения	Методы оценивания
В результате изучения курса студент будет знать методы трансляции, основанные на теории формальных грамматик, уметь создать грамматику нужного типа и выбрать нужную стратегию, знать и уметь реализовать все этапы построения компилятора.	• Лекции • Лабораторные работы	Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет с оценкой	Часы СРС	Задания
1. Введение. Основные понятия	4		3			2	Изучение учебного материала
2. Методы восходящего анализа	28		29			2	Изучение учебного материала
Подготовка к промежуточной аттестации в форме экзамена						0,55	
Прохождение промежуточной аттестации в форме зачета				3,2	0,25		
Всего	32		32	3,2	0,25	4,55	

Оценивание

Вид работы	Удельный вес (*в итоговой оценке,* %)	Период	Критерии оценки
Зачет	100	В конце семестра	Выполненные лабораторные работы

Литература

Основная литература:

- Компиляторы: принципы, технологии и инструментарий / Альфред В. Ахо, Миника С. Лам, Рави Сети,

Джеффри Д. Ульман ; [пер. с англ. и общ. ред. И. В. Красикова]. - 2-е изд. - Москва [и др.] : Вильямс, 2011. – 1175 с.

- Гагарина Л.Г. Введение в теорию алгоритмических языков и компиляторов : учебное пособие. /Л. Г. Гагарина, Е. В. Кокорева – М:Форум, 2013. – 175 с.
- Гавриков М. М. Теоретические основы разработки и реализации языков программирования : учебное пособие./М. М. Гавриков, А. Н. Иванченко, Д. В. Гринченков -М: Кнорус, 2016. – 177 с.

Дополнительная литература:

1. Ахо А., Ульман Дж. Теория синтаксического анализа, перевода и компиляции. Т 1, 2. М.: Мир, 1978 – 612 с., 486 с.
2. Лебедев В.Н. Введение в системы программирования. М.: Статистика, 1975 – 312 с.
3. Мозговой М.В. Классика программирования: алгоритмы, языки, автоматы, компиляторы. Практический подход. Санкт-Петербург: Наука и Техника, 2006 – 320 с.

Дополнительные рекомендации к дисциплине

Базы данных и информационно-справочные системы, в том числе зарубежные

1. Курс «Формальные языки и грамматики» Авторы: Ю. А. Макушин, Ю.А. Васильев (www.intuit.ru/studies/courses/108/108/lecture/3159
2. Курс "Основы разработки трансляторов". Автор: Легалов А.И. (http://www.softcraft.ru/translat/lect/content.shtml)
3. Языки программирования, формальные грамматики, конечные автоматы и методы трансляции Электронный ресурс : учебное пособие /Л. В. Горчаков ; Том. гос. ун-т, [Ин-т дистанционного образования]

Б1.В.08 Введение в специальность 1
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	1 курс 2 семестр	Вариативная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Информатика Введение в математику Дискретная математика	Алгебра Информатика

Цель и задачи дисциплины

Цель: формирование способности полноценного и увлеченного освоения базовых дисциплин профессионального цикла, в частности криптографических методов защиты информации.

Задачи:

- дать общие сведения об области и видах профессиональной деятельности;
- дать общие сведения о проблематике и методах защиты информации;
- ознакомить с основными понятиями и задачами криптографии;
- ознакомить с классическими шифрами и методах их криптоанализа.

Результаты обучения	Методы обучения	Методы оценивания
В результате изучения дисциплины студент должен **знать:** - основные понятия и задачи криптографии - способы и виды защиты информации **уметь:** - самостоятельно изучать и программно реализовывать простейшие криптографические алгоритмы **владеть:** - базовыми понятиями компьютерной безопасности	• Лекции	• Зачет с оценкой

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет с оценкой	Часы СРС	Задания
Предметная область компьютерной безопасности	8					20	Изучение учебного материала.
Введение в криптографию	8					22	Изучение учебного материала.
Классические (исторические) шифры и их криптоанализ	16					32,15	Изучение учебного материала.
Подготовка к зачету с оценкой				1,6			
Прохождение промежуточной аттестации в форме зачета с оценкой					0,25		
Всего	32			1,6	0,25	74,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет с оценкой	100%	В конце семестра	Отлично – студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении тестовых заданий. Хорошо – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении тестовых заданий. Удовлетворительно – студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении тестовых заданий. Неудовлетворительно – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении тестовых заданий.

Литература

1. Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата: [для студентов вузов, обучающихся по инженерно-техническим направлениям и специальностям] / И. Н. Васильева; С.-Петерб. гос. эконом. ун-т. Москва: Юрайт, 2016, 348 с.
2. Запечников С.В. Криптографические методы защиты информации: учебное пособие для академического бакалавриата: [для студентов вузов по направлению подготовки "Прикладная информатика" (квалификация бакалавр), по техническим направлениям и специальностям] / С. В. Запечников, О. В. Казарин, А. А. Тарасов. Москва: Юрайт, 2016, 308 с.

Дополнительные рекомендации к дисциплине

1. Сингх С. Книга шифров: тайная история шифров и их расшифровки. М.: АСТ, Астрель, 2007, 447 с.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. М.: Гелиос АРВ, 2002, 480 с.
3. Черчхаус Р. Коды и шифры. Юлий Цезарь, Энигма и Интернет. М.: Весь мир, 2005, 320 с.
4. Смарт Н. Криптография. М.: Техносфера, 2005, 528 с.
5. Stamp M., Iow R.M. Applied cryptanalysis. Breaking ciphers in the real world. – John Wiley and Sons, 2007, 401 pp.
6. Курс "Основы криптографии" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/691/547/info
7. Курс "Математика криптографии и теория шифрования" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/552/408/info
8. Курс "Криптографические основы безопасности" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/28/28/info

Б1.В.09 Введение в специальность 2
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	2 курс 3 семестр	Вариативная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Информатика Введение в математику Дискретная математика	Языки программирования Аппаратные средства вычислительной техники

Цель и задачи дисциплины

Цель: формирование способности полноценного и увлеченного освоения базовых дисциплин профессионального цикла через ознакомление с основными проблемами, задачами, областями, разделами, направлениями, методами компьютерной безопасности.

Задачи:

- дать знание терминологического и понятийного аппарата компьютерной безопасности
- сформировать представление о проблеме обеспечении безопасности компьютерных систем и сетей
- дать представление об общих принципах построения безопасных компьютерных систем и сетей

Результаты обучения	Методы обучения	Методы оценивания
В результате изучения дисциплины студент должен **знать:** - предметную область компьютерной безопасности **уметь:** - разрабатывать прототипы простейших средств защиты информации **владеть:** - понятийным аппаратом компьютерной безопасности - базовыми методами компьютерной безопасности	• Лекции	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Введение в компьютерную безопасность	8					8	Изучение учебного материала.
Модели управления доступом и информационными потоками	8					10	Изучение учебного материала.
Обзор классических атак на компьютерные системы	8					10	Изучение учебного материала.
Методы анализа безопасности компьютерных систем	8					10,15	Изучение учебного материала.
Подготовка к зачету с оценкой				1,6			
Прохождение промежуточной аттестации в форме зачета с					0,25		

оценкой							
Всего	32		1,6	0,25		38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	Отлично – студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении тестовых заданий. Хорошо – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении тестовых заданий. Удовлетворительно – студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении тестовых заданий. Неудовлетворительно – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении тестовых заданий.

Литература

1. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - Москва : ДМК Пресс, 2012. - 592 с.
2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. М: Книжный мир, 2009. 352 с.
3. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7, 2002, 1084 p.

Дополнительные рекомендации к дисциплине

1. Страница курса на Github: https://github.com/tsu-iscd/introduction-to-computer-security
2. Кочетков В. Философия Application Security. URL: https://www.youtube.com/watch?v=mb7tcT-9VXk
3. Кочетков В.. Прикладная теория безопасности приложений.
URL: https://my.webinar.ru/record/622509/?i=574d3d07f32978b0ae039c8604b45409

Б1.В.ДВ.01.01 Теория вычислительной сложности
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	4 курс 8семестр	Вариативная часть, дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
Андреева Валентина Валерьевна, к. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Введение в математику, Математический анализ, Алгебра, Дискретная математика, Математическая логика и теория алгоритмов, Теория вероятностей и математическая статистика, Информатика, Теоретико-числовые методы в криптографии, Английский язык	

Цель и задачи дисциплины		
Способность оценивать вычислительную сложность алгоритмов в системах защиты информации.		
Результаты обучения	**Методы обучения**	**Методы оценивания**
Обучающийся должен **знать** математический аппарат для оценки сложности алгоритмов и уметь его применять к алгоритмам в системах защиты информации.	• Лекции • Практические занятия.	• Экзамен

Содержание дисциплины							
Темы занятий	**Контактные часы**					**Самостоятельная работа**	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Сложность алгоритмов	2					2	Изучение учебного материала. Подготовка к практическим занятиям
Асимптотические оценки сложности алгоритмов	2					2	Изучение учебного материала.
Машины Тьюринга и другие модели	2	2					Изучение учебного материала. Подготовка к практическим занятиям
Языки и задачи	2	2				2	Изучение учебного материала. Подготовка к практическим занятиям
Неразрешимые задачи	2					2	
Трудно-решаемые задачи	2						
Основные сложностные классы алгоритмов	2						
Классы P и NP	2	2		0,5		4	Изучение учебного материала. Подготовка к практическим занятиям
NP- полные задачи	2	2				4	Изучение учебного материала. Подготовка к практическим занятиям
NP-полнота задач выполнимости КНФ	2	4		1		2	Изучение учебного материала. Подготовка к практическим занятиям
Другие NP- полные задачи	2	4		0,5		3,6	Изучение учебного материала. Подготовка к практическим занятиям

Параметризованные алгоритмы	2						
Генерическая сложность и генерическая разрешимость	2						
Генерическая сложность задачи останова МТ	2						
Абсолютно-неразрешимые задачи	2						
Генерическая сложность дискретного логарифмирования	2						
Подготовка к экзамену				2,4		33,7	
Сдача промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	16		4,4	0,3	55,3	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Практические занятия	50%	В течение семестра	Решение практических задач.
Экзамен	50%	В конце семестра	Знание теоретического материала и умение применить изученные методы и подходы к решению задач

Литература

1. Ахо А., Хопкрофт Дж., Ульман Дж.Построение и Анализ Вычислительных алгоритмов -М.: Мир, 1979.- 536 с.
2. Хопкрофт Дж., Мотвани Р., Ульман Дж. Ведение в теорию автоматов языков и вычислений.2-е издание.- М.: Издательский дом "Вильямс", 2002.- 528 с.
3. A.G. Myasnikov and A.N.Rybalov Generic Complexity of Undeciable Problems. -The Journal of Symbolic Logic, vol.73 (June 2008), no. 2, pp.656-673.
4. D.Hamkin and A. D. Miasnikov The Halting Problem Is Decidable On a Set of Asymptotic Probability One.- Notre DamaJournal of Formal Logic, vol. 47 (2006), no.4, pp. 515-524.

Дополнительные рекомендации к дисциплине

1. Рыбалов А Н О генерической сложности проблемы дискретного логарифма Прикладная дискретная математика. 2016, №3 (33), С. 93-97.
2. Быкова В.В. алгоритмы иих классификация на основе эластичности. Прикладная дискретная математика. 2011, №4, С.1- 9.
3. Агибалов Г. П. Теория вычислительной сложности. Конспект лекций. 2016. Электронный ресурс кафедры

Б1.В.ДВ.01.02 Алгоритмические системы
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	4 курс 8семестр	Вариативная часть, дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Введение в математику, Математическая логика и теория алгоритмов, Информатика	

Цель и задачи дисциплины		
Цель: познакомить обучающихся с основными понятиями теории алгоритмов, научить записывать алгоритмы в различных алгоритмических системах.		
Результаты обучения	**Методы обучения**	**Методы оценивания**
Обучающийся должен **знать** основные понятия теории алгоритмов; **уметь** записывать алгоритмы в различных алгоритмических системах, разрабатывать, реализовывать, отлаживать и оптимизировать алгоритмы; **владеть** навыками алгоритмического мышления	• Лекции • Самостоятельная работа.	• Экзамен

Содержание дисциплины							
Темы занятий	**Контактные часы**					**Самостоятельная работа**	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Алгоритмы н алгоритмические системы	2					1	Изучение учебного материала.
Классы и свойства алгоритмов	2					1	Изучение учебного материала.
Нормальные алгорифмы Маркова – определение	2	4				2	Изучение учебного материала. Подготовка к практическим занятиям
Композиции нормальных алгорифмов Маркова	2					1	Изучение учебного материала
Универсальный нормальный алгорифм Маркова	2					1	Изучение учебного материала
Принцип нормализации	2					1	Изучение учебного материала
Машины Тьюринга	2	4				2	Изучение учебного материала. Подготовка к практическим занятиям
Композиции машин Тьюринга	2					1	Изучение учебного материала
Основная гипотеза теории алгоритмов	2					1	Изучение учебного материала
Универсальная машина Тьюринга	2	4				2	Изучение учебного материала. Подготовка к практическим занятиям
Алгоритмическая неразрешимость проблемы применимости	2					2	Изучение учебного материала
Машина Поста	2	4				2	Изучение учебного материала.

							Подготовка к практическим занятиям
Примитивно рекурсивные функции	2	4				1,6	Изучение учебного материала
Частично рекурсивные функции	2					1	Изучение учебного материала
Тезис Черча	2					1	Изучение учебного материала
Эквивалентность алгоритмических систем	2					1	Изучение учебного материала
Подготовка к экзамену				2,4		33,7	
Сдача промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	16		4,4	0,3	55,3	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Практические занятия	50%	В течение семестра	Решение практических задач.
Экзамен	50%	В конце семестра	Знание теоретического материала и умение применить изученные методы и подходы к решению задач

Литература

1. Панкратова И.А., Сибирякова В.А. Алгоритмические системы. Томск: И У, 2009.
2. Мальцев А.И. Алгоритмы и рекурсивные функции. М.: Физматлит, 1986.
3. Успенский В.А. Машина Поста. М.: Наука, 1988.
4. Трахтенброт Б.А. Алгоритмы и машинное решение задач. М.: Физматлит, 1960.
5. Алферова З.В. Теория алгоритмов. М.: Статистика, 1973.

Б1.В.ДВ.02.01 Квантовые вычисления
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	5 курс А семестр	Дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Информатика, Алгебра, Дискретная математика Языки программирования, Математическая логика и теория алгоритмов, Теория вероятностей и математическая статистика, Криптографические методы защиты информации, Теория кодирования, сжатия и восстановления информации	Криптографические протоколы Облачные вычисления Постквантовая криптография Методы верификации

Цель и задачи дисциплины

Цель: формирование способности изучения и анализа квантовых алгоритмов

Задачи:

- дать общие сведения о квантовых вычислениях
- ознакомить с основными квантовыми алгоритмами
- дать основы квантовой криптографии

Результаты обучения	Методы обучения	Методы оценивания
В результате изучения дисциплины студент должен **знать:** - математические основы квантовых вычислений - основные квантовые алгоритмы **уметь:** - проводить синтез и анализ квантовых схем **владеть:** - инструментами симулирования квантовых схем	• Лекции	• Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Введение в квантовые вычисления	8					8	Изучение учебного материала.
Квантовые схемы	8					8	Изучение учебного материала
Квантовые алгоритмы	8					14,4	Изучение учебного материала.
Квантовые протоколы	8					8	Изучение учебного материала.
Подготовка к экзамену				1,6		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32			3,6	0,3	72,1	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100%	В конце семестра	Отлично – студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении тестовых заданий. Хорошо – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении тестовых заданий. Удовлетворительно – студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении тестовых заданий. Неудовлетворительно – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении тестовых заданий.

Литература

1. Райли Т. Перри Элементарное введение в квантовые вычисления. Учебное пособие / Пер. с англ. А. Д. Калашникова. - М.: Интеллект, 2015.- 208 с.
2. Альбов А.С. Квантовая криптография /Александр Альбов. - Санкт-Петербург: Страта, 2015. -248 с.

Дополнительные рекомендации к дисциплине

1. Кайе Ф., Лафламм Р., Моска М. Введение в квантовые вычисления / Ф.Кайе. – Пер. с англ. Т. С. Никитиной под науч. ред. А. В. Анохина. Москва, Ижевск: Регулярная и хаотическая динамика, Ижевский институт компьютерных исследований, 2009, 360 с.
2. Имре Ш., Баланж Ф. Квантовые вычисления и связь. Инженерный подход / Ш. Имре. Пер. с англ. под редакцией В.В.Самарцева. М. : ФИЗМАТЛИТ, 2008. – 320 с.
3. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация / М. Нильсен . М.: Мир, 2006, 824 с.
4. Валиев К., Кокин А.А. Квантовые компьютеры: надежды и реальность / К. Валиев. Ижевск: РХД, 2004, 320 с.
5. Ожигов Ю.И. Квантовые вычисления / Ю.И. Ожигов. М.: Макс Пресс, 2003, 152 с.
6. Курс "Классические и квантовые вычисления" [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ". URL: http://www.intuit.ru/studies/courses/1057/136/info
7. Ллойд С. Квантовые вычисления (видео) [Электронный ресурс] // ПостНаука - интернет-журнал о современной фундаментальной науке. URL: https://postnauka.ru/video/54343

Б1.В.ДВ.02.02 Алгебраические системы
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
3 з.е.	специалитет	5 курс 10 семестр	Вариативная часть, дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Введение в математику	

Цель и задачи дисциплины

Цель: познакомить обучающихся с основными понятиями теории алгебраических систем и научить применять теорию алгебраических систем при анализе криптографических систем защиты информации.

Результаты обучения	Методы обучения	Методы оценивания
Обучающийся должен **знать** основы теории алгебраических систем и уметь его применять в анализе и синтезе криптографических систем защиты информации.	• Лекции • Самостоятельная работа.	• Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Общие понятия. Отношения и отображения: множества 2) отношения, 3) отображения, 4) эквивалентности, 5) частичные и линейные порядки 6) многозначные и частичные отображения.	4					6	Изучение учебного материала.
Модели и алгебры 1) n-арные отношения и функции, 2) алгебраические системы, 3) подсистемы, порождающие совокупности, 4) конгруенции, 5) декартовы произведения, 5) операции над кардинальными и порядковыми числами.	6					6	Изучение учебного материала.
Классические алгебры. Группоиды и группы: 1) группоиды и полугруппы, 2) квазигруппы и лупы, 3) группы.	6					6	Изучение учебного материала.
Кольца и тела: 1) кольца, 2) алгебраически замкнутые поля, 3) альтернативные тела, 4) линейные алгебры.	4					6	Изучение учебного материала.
Решетки: 1) решетки, 2) модулярные и дистрибутивные	6					6	Изучение учебного материала

решетки, 3) Булевы алгебры							
Языки первой и второй ступени. Синтаксис и семантика: 1) теоремы, 2) формулы, 3) свойства 2-й ступени, 4) элементарные теории и аксиоматизируемые классы, 5) классификация формул	6					8,4	Изучение учебного материала
Подготовка к экзамену				1,6		33,7	
Сдача промежуточной аттестации в форме экзамена				2	0,3		
Всего	32			3,6	0,3	72,1	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Экзамен	100%	В конце семестра	Знание и понимание материала в полном объеме - отлично Хорошее знание материала за исключением некоторых деталей - хорошо. Неглубокое понимание на уровне общих представлений - удовлетворительно.

Литература

Мальцев А.И. Алгебраические системы. М.: Наука, 1970. – 392 с.

Дополнительные рекомендации к дисциплине

1. Helena Rasiova. Introduction to modern mathematics. Amsterdam-London-Warszawa. 1973. – 339 p.

Б1.В.ДВ.03.01 Облачные вычисления
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	5 курс 10 семестр	Обязательная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Самохина Светлана Ивановна, к.ф.-м.н., доцент	Кафедра компьютерной безопасности ИПМКН

Пререквизиты	Параллельно осваиваемые дисциплины
Информатика, алгоритмы и структуры данных, современные компьютерные технологии.	Сети и системы передачи информации, безопасность веб-приложений, научно-исследовательская работа.

Цель и задачи дисциплины

Цель и задачи дисциплины – получение общих сведений об облачных вычислениях, предпосылках его развития, основных моделях облачных технологий, необходимых для решения различных задач практической и научно-исследовательской деятельности.

Результаты обучения	Методы обучения	Методы оценивания
Обучающийся узнает архитектуру и сетевые модели облачных сервисов, получит сведения об особенностях проектирования облачных архитектур. Способен спроектировать программное обеспечение, связанное с облачными вычислениями и написать программный код, а также проверить работоспособность программного обеспечения и исправить дефекты.	• Лекции • Самостоятельная работа	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Введение в Облачные технологии. Общие сведения	2						Изучение учебного материала
Доклад с презентацией	6						Подготовка доклада
Обзор облачных архитектур	2						Изучение учебного материала
Сетевые модели облачных сервисов	2						Изучение учебного материала
Технологии виртуализации	2						Изучение учебного материала
Особенности и основные аспекты проектирования облачных архитектур	2						Изучение учебного материала
Основные PaaS-платформы	2						Изучение учебного материала
Работа с Google-технологиями Программа с использованием данных, расположенныех в облаке	12						Изучение учебного материала
Вирусы и антивирусы	2						Изучение учебного материала

Изучение учебного материала, подготовка к практическим занятиям Подготовка к сдаче зачета						38,15	
Промежуточная аттестация в форме зачета с оценкой				1,6	0,25		
Всего	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	**Зачтено**: студент владеет большей частью теоретического материала, но имеет некоторые проблемы в знаниях, допускает негрубые ошибки; **Незачтено**: студент не освоил большую часть теоретического материала.

Литература

1. Елисеев А. С. Сочетание GRID-технологий и облачных вычислений для выполнения сложных математических расчетов / А. С. Елисеев // Инноватика - 2017 : сборник материалов XIII Международной школы-конференции студентов, аспирантов и молодых ученых, 20–22 апреля 2017 г., г. Томск, Россия. Томск, 2017. С. 361-364. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000626192
2. От хранения данных к управлению информацией : [учебник для студентов вузов по направлениям подготовки 09.03.02 "Информационные системы и технологии (уровень бакалавриата)" и 09.04.02 "Информационные системы и технологии (уровень магистратуры)" / ред.: Гнанасундарам Сомасундарам, Алок Шривастава]. - 2-е изд.. - Санкт-Петербург [и др.] : Питер, 2016. - 543 с.: рис.
3. Риз Д. Облачные вычисления / Джордж Риз ; [пер. с англ. О. Кокоревой ; гл. ред. Е. Кондукова]. - Санкт-Петербург : БХВ-Петербург, 2011. - 1 онлайн-ресурс (278 с.): ил., табл.. URL: http://sun.tsu.ru/limit/2017/000556255/000556255.pdf
4. "Облачные" сервисы высокопроизводительных вычислительных ресурсов для образования, науки и промышленности / В. П. Демкин, А. В. Борисов, С. А. Орлов, В. Н. Руденко // Открытое и дистанционное образование. 2012. № 2 (46). С. 16-23. URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000446752

Б1.В.ДВ.03.02 Постквантовая криптография
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	специалитет	5 курс А семестр	Дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Теория вероятностей и математическая статистика, Дискретная математика Теория чисел, Алгебра, Теоретико-числовые методы в криптографии, Криптографические методы защиты информации, Булевы функции в криптографии, Профессиональный перевод специальной литературы, Теория кодирования, сжатия и восстановления информации	Криптографические протоколы Аппаратная реализация криптоалгоритмов

Цель и задачи дисциплины

Цель: формирование общих представлений об алгоритмах постквантовой криптографии

Задачи:

- дать представление об основных конструкциях постквантовой криптографии и их стойкости
- ознакомить с проектом NIST по стандартизации постквантовой криптографии

Результаты обучения	Методы обучения	Методы оценивания
В результате изучения дисциплины студент должен **знать:** - основные конструкции постквантовой криптографии **уметь:** - применять математические методы при исследовании алгоритмов постквантовой криптографии **владеть:** - понятийным аппаратом постквантовой криптографии	• Лекции	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Введение в постквантовую криптографию	4					7	Изучение учебного материала.
Постквантовая криптография на основе решёток	8					8	Изучение учебного материала.
Постквантовая криптография на основе кодов	8					8	Изучение учебного материала.
Криптография на основе хеш-функций	4					7	Изучение учебного материала.
Стандартизация постквантовой	8					8,15	Изучение учебного материала.

криптографии							
Подготовка к зачету с оценкой				1,6			
Прохождение промежуточной аттестации в форме зачета с оценкой					0,25		
Всего	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	Отлично – студент в совершенстве овладел всеми теоретическими вопросами обязательного материала по разделам лекционного курса, показал все требуемые умения и навыки при выполнении тестовых заданий. Хорошо – студент овладел обязательным материалом по разделам лекционного курса, возможно с некоторыми недостатками, а также показал все требуемые умения и навыки при выполнении тестовых заданий. Удовлетворительно – студент имеет недостаточно глубокие знания по теоретическим разделам обязательного материала дисциплины, но показал все требуемые умения и навыки при выполнении тестовых заданий. Неудовлетворительно – студент имеет существенные пробелы по отдельным теоретическим разделам дисциплины или не показал требуемые умения и навыки при выполнении тестовых заданий.

Литература

1. Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen Post-Quantum Cryptography. Springer, 2009, 246 pages
2. Комарова А.В., Коробейников А.Г. Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности - 2019. - № 2(30). - С. 58-68
3. Шокуров А.В., Кузюрин Н.Н., Фомин С.А. Решетки, алгоритмы и современная криптография. М.: Институт системного программирования РАН, 2011. 130 с.

Дополнительные рекомендации к дисциплине

1. Проект NIST по стандартизации постквантовой криптографии – https://csrc.nist.gov/projects/post-quantum-cryptography
2. Post-quantum cryptography - https://pqcrypto.org/
3. Буковшин В.А., Чуб П.А., Черкесова Л.В., Короченцев Д.А., Поркшеян В.М. Анализ современных покстквантовых алгоритмов шифрования // Научное обозрение. Технические науки. – 2019. – № 4. – С.36-44; URL: https://science-engineering.ru/ru/article/view?id=1254

Б1.В.ДВ.04.01 Технология разработки программ
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
5 з.е	специалитет	3 курс 5 семестр	Вариативная часть, дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
Андреева Валентина Валерьевна, к.т.н, доцент	Кафедра компьютерной безопасности, ИПМКН

Пререквизиты	Параллельно осваиваемые дисциплины
«Информатика», «Алгоритмы и структуры данных I, II»	«Языки программирования»

Цель и задачи дисциплины		
Цель дисциплины ознакомить студентов с основными технологиями, принципами, методами и методологиями разработки системного и прикладного программного обеспечения. А также формирование устойчивых навыков объектно-ориентированного анализа, проектирования и программирования (OOA/OOD/OOP).		
Результаты обучения	**Методы обучения**	**Методы оценивания**
Знание технологий, методов разработки системного и прикладного программного обеспечения.	• Лекции • Практические занятия • Лабораторные работы	Экзамен

Содержание дисциплины							
Темы занятий	**Контактные часы**					**Самостоятельная работа**	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Объектно-ориентированный подход к разработке ПО	3					4	Изучение лекционного материала.
Основные понятия и принципы построения объектно-ориентированных систем. Теории классификации.	4					4	Изучение лекционного материала.
Реализация практической задачи в соответствии объектно-ориентированными принципами.		14	14			4	Изучение методов. Подготовка к лабораторным работам.
Паттерны проектирования – общий обзор. Порождающие паттерны. Структурные паттерны. Паттерны поведения	8					6	Изучение лекционного материала.
Реализация практической задачи с применением изученных паттернов.		10	10			4	Изучение методов. Подготовка к лабораторным работам.
GRASP паттерны	4					3	Изучение методов. Подготовка к лабораторным работам.

Реализация практической задачи с применением изученных паттернов.		8	8			4	Подготовка к лабораторным работам.
Методологии разработки программного обеспечения – общий обзор.	2					2	Изучение лекционного материала.
Методология Rational Unified Process (RUP).	8					4	Изучение лекционного материала.
Гибкие методологии разработки. Agile. Scrum и Kanban.	2					4	Изучение лекционного материала.
Методологии управления проектами.	12					4,2	Изучение лекционного материала.
Подготовка к промежуточной аттестации в форме экзамена				4,8		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	32	32	6,8	0,3	76,9	

Оценивание			
Вид работы	**Удельный вес** (*в итоговой оценке, %*)	**Период**	**Критерии оценки**
1. Лабораторные работы	50%	в течении семестра	Реализация предложенных задач.
2. Экзамен	50%	в конце семестра	Знание теоретического материала и умение применить изученные методы и подходы к проектированию программного обеспечения.

Литература

- **Основная литература:**

1. Страуструп Б. Программирование. Принципы и практика использования C++, 1238 с. Вильямс2011.
2. Затонский А. В. Информационные технологии. Разработка информационных моделей и систем: учебное пособие: [для студентов вузов, обучающихся по направлению 230100 "Информатика и вычислительная техника"], 343 с. Москва: ИНФРА-М 2014.
3. Орлов С. А. Технологии разработки программного обеспечения: современный курс по программной инженерии: [учебник для студентов вузов, обучающихся по специальности "Программное обеспечение вычислительной техники и автоматизированных систем" направлений подготовки дипломированных специалистов "Информатика и вычислительная техника"], 608 с. Питер 2012.

- **Дополнительная литература**

4. Гради Буч, Роберт А. Максимчук, Майкл У. Энгл Объектно-ориентированный анализ и проектирование с примерами приложений, 718 с. Вильямс 2010
5. Мирютов А. А. Программная инженерия: учебно-методический комплекс [Электронный ресурс], URL: http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000462187, ИДО ТГУ 2012

Дополнительные рекомендации к дисциплине

Базы данных и информационно-справочные системы, в том числе зарубежные

1. Издательство «Лань» [Электронный ресурс] : электрон.-библиотечная система. – Электрон. Дан. – СПб., 2010. – URL: http://e.lanbook.com/
2. ScienceDirect [Electronic resource] / Elsevier B.V. – Electronic data. – Amsterdam, Netherlands, 2016. – URL: http://www.sciencedirect.com/
3. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. – Электрон. Дан. – М., 2000. – URL: http://elibrary/ru/defaultx.asp?

Б1.В.ДВ.04.02 Промышленное программирование
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
5 з.е	специалитет	3 курс 5 семестр	Вариативная часть, дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
	Кафедра компьютерной безопасности, ИПМКН

Пререквизиты	Параллельно осваиваемые дисциплины
«Информатика», «Алгоритмы и структуры данных I, II»	«Языки программирования»

Цель и задачи дисциплины

Цель дисциплины ознакомить студентов с основными технологиями, принципами и методами разработки программного обеспечения.

Результаты обучения	Методы обучения	Методы оценивания
Знать этапы создания автоматизированной системы; разновидности процесса разработки программ; основы языка проектирования UML; основные объектно-ориентированные шаблоны проектирования ПО; классификацию основных типов архитектур ПО. **Уметь** составлять проектную документацию на различных этапах создания ПО; осуществлять процесс верификации и валидации программ; производить оценку сложности проекта; **Владеть** навыками коллективной разработки программ, навыками работы с системами управления исходными текстами и процессом разработки ПО.	• Лекции • Практические занятия • Лабораторные работы	Экзамен

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Экзамен	Часы СРС	Задания
Языки безопасного программирования	12	12	12			15	Изучение лекционного материала. Подготовка к занятиям
Защита программ от исследования	10	10	10			15	Изучение лекционного материала. Подготовка к занятиям
Тестирование программного обеспечения.	10	10	10			13,2	Изучение методов. Подготовка к занятиям
Подготовка к промежуточной аттестации в форме экзамена				4,8		33,7	
Прохождение промежуточной аттестации в форме экзамена				2	0,3		
Всего	32	32	32	6,8	0,3	76,9	

Оценивание			
Вид работы	**Удельный вес** (*в итоговой оценке, %*)	**Период**	**Критерии оценки**
1. Лабораторные работы	50%	в течении семестра	Реализация предложенных задач.
2. Экзамен	50%	в конце семестра	Знание теоретического материала и умение применить изученные методы и подходы к проектированию программного обеспечения.

Литература

- **Основная литература:**

1. Фаулер М. UML. Основы. Краткое руководство по стандартному языку объектного моделирования. – М.: Символ-плюс, 2011 - 192 с.
2. Макконнелл С. Совершенный код. Мастер-класс - М.: Русская Редакция, 2010 – 896 с.
3. Орлов С. А. Технологии разработки программного обеспечения: современный курс по программной инженерии: [учебник для студентов вузов, обучающихся по специальности "Программное обеспечение вычислительной техники и автоматизированных систем" направлений подготовки дипломированных специалистов "Информатика и вычислительная техника"], 608 с. Питер 2012.

- **Дополнительная литература**

4. Брауде Э. Дж. Технологии разработки программного обеспечения.,– СПб.: Питер, 2004 -656с
5. Гамма Э., Хелм Р., Джонсон Р., Влиссидес Дж. Приёмы объектно-ориентированного проектирования. Паттерны проектирования – СПб.: Питер, 2007 - 366 с.

Б1.В.ДВ.05.01 Спецсеминар АБКС
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
8 з.е.	специалитет	3 курс 5 семестр 4 курс 7 семестр 5 курс 10 семестр 6 курс 11 семестр	Вариативная часть, дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
Останин Сергей Александрович, канд. техн. наук, доцент Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Дискретная математика Алгебра Введение в математику Алгоритмы и структуры данных I, II Введение в специальность Криптографические методы защиты информации Алгоритмы кодирования и сжатия информации	Математическая логика и теория алгоритмов Дискретная математика. Теория автоматов Булевы функции в криптографии

Цель и задачи дисциплины

Цель: Семинар служит для обсуждения научных результатов, относящихся к общей тематике «Анализ безопасности компьютерных систем». На семинаре студенты делают доклады по результатам собственных исследований в этой области, выполняемых ими под руководством преподавателя

Задачи:

- Самостоятельно планировать научно- исследовательскую работу
- Владеть методами планирования и организации научно- исследовательской работы
- Знать основные источники научно-технической информации, методических материалов, нормативных правовых актов в сфере профессиональной деятельности;
- Уметь осуществлять подбор научно-технической информации, методических материалов и нормативных правовых агатов в сфере профессиональной деятельности
- Владеть навыками изучения и обобщения научно-технической информации, методических материалов и нормативных правовых актов в сфере профессиональной деятельности

Результаты обучения	Методы обучения	Методы оценивания
Формирование у студентов профессиональных компетенций в соответствии с ФГОС ВО по специальности *Компьютерная безопасность*. Результат оформляется в виде научно-исследовательской работы.	• Семинары	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Семестр 5/ 7/ 10/ 11							
1. Обзор актуальных направлений		2				6	Изучение учебного материала.

исследований							Подготовка к семинарам (подготовка доклада по результатам научных исследований)
2. Постановка задачи		4				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
3. Обзор известных методов		6				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
4. Формулировка и обоснование метода решения		8				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
5. Основные результаты		8				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
6. Рекомендации по практическому применению результатов, перспективы дальнейших исследований		4				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
Подготовка к промежуточной аттестации в форме зачета				1,6		2,15	
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего за семестр		32		1,6	0,25	38,15	
Итого		128		6,4	1	152,6	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
- Проект - Зачет -	100	В течение семестра В конце семестра	**Зачтено** – уверенно ориентируется в рассматриваемой тематике **Незачтено** – плохо ориентируется в рассматриваемой тематике

Литература

1. Кузнецов И. Н. Научное исследование: методика проведения и оформление. - 3-е изд., перераб. и доп. - М.: Дашков и К*, 2008. - 460 с.
2. Основы научных исследований: учеб, пособие. - М.: Форум, 2009. - 272 с.

Дополнительные рекомендации к дисциплине

дополнительная литература:

1.Теплицкая, Т. Ю. Научный и технический текст: правила составления и оформления. - Ростов н/Д. : Феникс, 2007. - 156 с.

Б1.В.ДВ.05.02 Спецсеминар ММЗИ
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
8 з.е.	специалитет	3 курс 5 семестр 4 курс 7 семестр 5 курс 10 семестр 6 курс 11 семестр	Вариативная часть, дисциплина по выбору	Очное обучение	Русский

Преподаватель	Структурное подразделение
Останин Сергей Александрович, канд. техн. наук, доцент Тренькаев Вадим Николаевич, канд. техн. наук, доцент	Кафедра компьютерной безопасности

Пререквизиты	Параллельно осваиваемые дисциплины
Дискретная математика Алгебра Введение в математику Алгоритмы и структуры данных I, II Введение в специальность Криптографические методы защиты информации Алгоритмы кодирования и сжатия информации	Математическая логика и теория алгоритмов Дискретная математика. Теория автоматов Булевы функции в криптографии

Цель и задачи дисциплины

Цель: Семинар служит для обсуждения научных результатов, относящихся к общей тематике «Анализ безопасности компьютерных систем». На семинаре студенты делают доклады по результатам собственных исследований в этой области, выполняемых ими под руководством преподавателя

Задачи:

- Самостоятельно планировать научно- исследовательскую работу
- Владеть методами планирования и организации научно- исследовательской работы
- Знать основные источники научно-технической информации, методических материалов, нормативных правовых актов в сфере профессиональной деятельности;
- Уметь осуществлять подбор научно-технической информации, методических материалов и нормативных правовых агатов в сфере профессиональной деятельности
- Владеть навыками изучения и обобщения научно-технической информации, методических материалов и нормативных правовых актов в сфере профессиональной деятельности

Результаты обучения	Методы обучения	Методы оценивания
Формирование у студентов профессиональных компетенций в соответствии с ФГОС ВО по специальности *Компьютерная безопасность*. Результат оформляется в виде научно-исследовательской работы.	• Семинары	• Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Семинары	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Семестр 5/ 7/ 10/ 11							
1. Обзор актуальных направлений		2				6	Изучение учебного материала.

исследований							Подготовка к семинарам (подготовка доклада по результатам научных исследований)
2. Постановка задачи		4				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
3. Обзор известных методов		6				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
4. Формулировка и обоснование метода решения		8				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
5. Основные результаты		8				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
6. Рекомендации по практическому применению результатов, перспективы дальнейших исследований		4				6	Изучение учебного материала. Подготовка к семинарам (подготовка доклада по результатам научных исследований)
Подготовка к промежуточной аттестации в форме зачета				1,6		2,15	
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего за семестр		32		1,6	0,25	38,15	
Итого		128		6,4	1	152,6	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
- Проект - Зачет -	100	В течение семестра В конце семестра	**Зачтено** – уверенно ориентируется в рассматриваемой тематике **Незачтено** – плохо ориентируется в рассматриваемой тематике

Литература

1. Кузнецов И. Н. Научное исследование: методика проведения и оформление. - 3-е изд., перераб. и доп. - М.: Дашков и К*, 2008. - 460 с.
2. Основы научных исследований: учеб, пособие. - М.: Форум, 2009. - 272 с.

Дополнительные рекомендации к дисциплине

дополнительная литература:

2.Теплицкая, Т. Ю. Научный и технический текст: правила составления и оформления. - Ростов н/Д. : Феникс, 2007. - 156 с.

ФТД.01 Технология блокчейн
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
2 з.е.	Специалитет	4 курс 7 семестр	факультативная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Лавров Валерий Александрович	Институт прикладной математики и компьютерных наук, кафедра теоретических основ информатики

Пререквизиты	Параллельно осваиваемые дисциплины
Операционные системы	Компьютерные науки

Цель и задачи дисциплины

Изучение технологии блокчейн (распределенного реестра) с акцентом на её математические и технические основы, а также прикладные аспекты.

Результаты обучения	Методы обучения	Методы оценивания
ИОПК-2.2. Применяет знания, полученные в области информационных технологий и программных средств при решении задач профессиональной деятельности Способен спроектировать приложение от формулировки прикладной задачи до технического описания	• Лекции • Практики	• Тест • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
1. Основны блокчейна	8			0,4		9	Изучение теоретического материала по теме 1. Самостоятельное выполнение практической работы №1.
2. Криптографические основы блокчейна	8			0,4		9	Изучение теоретического материала по теме 2. Самостоятельное выполнение практической работы №2.
3. Умные контракты	8			0,4		9	Изучение теоретического материала по теме 3. Самостоятельное выполнение практической работы №3.
4. Приватные блокчейны	8			0,4		11,15	Изучение теоретического материала по теме 4. Самостоятельное выполнение практической работы №4.
Прохождение промежуточной					0,25		

аттестации в форме зачета							
Всего:	32			1,6	0,25	38,15	

Оценивание			
Вид работы	**Удельный вес**	**Период**	**Критерии оценки**
Зачет	100%	В конце семестра	**Зачтено**: студент полностью владеет теоретическим материалом; **Не зачтено**: студент не освоил большую часть теоретического материала.

Литература
Даниэль Дрешер Основы блокчейна: вводный курс для начинающих в 25 небольших главах. – ДМК Пресс, 2018. – 320 с.
Дополнительные рекомендации к дисциплине
Алексей Михеев, Артем Генкин Блокчейн: Как это работает и что ждет нас завтра. Альпина Паблишер, 2018. – 592 с.

ФТД.02 СУБД Oracle
Аннотация

Трудоемкость	Уровень	Период изучения	Вид дисциплины	Формат	Язык
1 з.е	специалитет	4 курс, 7семестр	факультативная	Очное обучение	Русский

Преподаватель	Структурное подразделение
Николаева Екатерина Александровна, к.т.н, доцент	Кафедра компьютерной безопасности ИПМКН

Пререквизиты	Параллельно осваиваемые дисциплины
«Информатика», «Дискретная математика», «Системы управления базами данных»	«Научно-исследовательская работа»

Цель и задачи дисциплины

Цель – формирование навыков программирования в СУБД ORACLE, а также знаний об основных управляющих конструкциях языка PL/SQL, структурах данных, основных приемах программирования PL/SQL

Результаты обучения	Методы обучения	Методы оценивания
Обучающийся сможет: - создавать хранимые программные единицы PL/SQL (процедуры, триггеры, отдельные сценарии и т.д.) направленные на решение прикладных задач в рамках существующих и (или) проектируемых БД; - сопровождать и дорабатывать существующие хранимые программные единицы PL/SQL; - исправлять дефекты разработанные самостоятельно и(или) переданных для сопровождения процедур и триггеров. - оформлять наспанный код в соответствии с существующими соглашениями. - выполнять разбор существующего кода написанного на PL/SQL с целью проведения рефакторинга и анализа возможности оптимизации.	• Лабораторные работы	• Тест • Проект • Зачет

Содержание дисциплины

Темы занятий	Контактные часы					Самостоятельная работа	
	Лекции	Практические занятия	Лабораторные занятия	Консультации	Зачет	Часы СРС	Задания
Язык PL-SQL. Основные управляющие конструкции языка PL-SQL.			2			2	Изучение материала занятия
Анонимные блоки. Процедуры и функции PL-SQL.			2			2,5	Изучение материала занятия
Курсоры.			2			2,5	Изучение материала занятия
Обработка исключений.			2			2	Изучение материала занятия
Модули.			2			2	Изучение материала занятия
Триггеры.			2			3	Изучение материала занятия

Объектные типы.			2			2	Изучение материала занятия
Динамический SQL.			2			2,95	Изучение материала занятия
Индивидуальные консультации в семестре				0,8			
Прохождение промежуточной аттестации в форме зачета					0,25		
Всего			16	0,8	0,25	18,95	

Оценивание			
Вид работы	**Удельный вес** (*в итоговой оценке, %*)	**Период**	**Критерии оценки**
Выполнение индивидуальных лабораторных работ	70%	В течение семестра	Правильное выполнение всех заданий
Итоговое тестирование Зачет	30%	В конце семестра	Выполнение не менее 60% заданий

Литература

1. Фейерштейн С., Прибыл Б. Oracle PL/SQL для профессионалов. 940 с. Санкт-Петербург: Питер - 2004.
2. Издательство «Лань» [Электронный ресурс] : электрон.-библиотечная система. – Электрон. Дан. – СПб., 2010. – URL: http://e.lanbook.com/
3. Oracle Help Center [Electronic resource] – URL: https://docs.oracle.com/database/121/LNPLS/toc.htm

Дополнительные рекомендации к дисциплине

Для достижения успеха в освоении дисциплины студент должен самостоятельно выполнять проектные работы, проявлять активность во время аудиторных занятий, демонстрировать способность решать поставленные задачи в оговоренные сроки и стремление оптимизировать предложенные решения, свободно владеть теоретическим мате риалом, изученным в рамках курса. Приветствуется самостоятельная работа с документацией. Работа с указанными преподавателем разделами документации настоятельно рекомендуется. Приветствуется работа с актуальными материалами из зарубежной профессиональной периодики, посвященными обсуждению реальных проблем построения и эксплуатации интеллектуальных алгоритмов в выбранной для самостоятельной работы предметной области.