ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Заведующий выпускающей кафедрой

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 10.07.2024

А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П1.06 Криптографические методы защиты информации
для направления 01.03.02 Прикладная математика и информатика
уровень Бакалавриат
профиль подготовки Математические методы обеспечения безопасности программных систем
форма обучения очная
кафедра-разработчик Прикладная математика и программирование

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 01.03.02 Прикладная математика и информатика, утверждённым приказом Минобрнауки от 10.01.2018 № 9

Зав.кафедрой разработчика, д.физ.-мат.н., проф.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 10.07.2024

А. А. Замышляева

Разработчик программы, д.физ.-мат.н., доц., профессор

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Зюляркина Н. Д.
Пользователь: ziuliarkinand
Дата подписания: 04.07.2024

Н. Д. Зюляркина

Челябинск

1. Цели и задачи дисциплины

Целью изучения дисциплины является формирование у студентов общих представлений о содержании криптографических методов защиты информации и о подходах к оценке эффективности таких методов. Задачи дисциплины: дать представление об информационной безопасности, как сфере профессиональной деятельности; раскрыть особенности криптографических методов защиты информации и содержание базовых понятий криптографии; ознакомить с основными видами шифров; ознакомить с современными стандартами криптографической защиты; дать представление об атаках на криптографические системы.

Краткое содержание дисциплины

В рамках данной дисциплины исследуются основные типы шифров, проводится анализ их криптостойкости, изучаются основные типы атак и методы противодействия им.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-6 Способен использовать математические методы при проектировании и разработке алгоритмических и программных решений в области обеспечения безопасности и защиты программных систем.	Знает: принципы построения криптографических алгоритмов, криптографические стандарты, основные подходы к реализации криптографических средств защиты информации Имеет практический опыт: решения задач, связанных с распределением ключевой информации, шифрованием чувствительной информации и цифровой подписью сообщений

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Математические основы криптографии, Теория информации и кодирования	Программные методы защиты информации, Математическое моделирование и прогнозирование информационных угроз, Квантовая криптография, Квантовые коммуникации и криптография, Криптографические протоколы

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Математические основы криптографии	Знает: алгебраические структуры, лежащие в основе современных криптографических систем Умеет: использовать математические методы при

	создании криптографических спецификаций Имеет практический опыт:
Теория информации и кодирования	Знает: способы формирования оптимальных кодов в системе передачи информации Умеет: Имеет практический опыт: оценки предельных возможностей информационных систем, оптимального кодирования и передачи сигналов

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 74,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	69,5	69,5
Написание программ, реализующих заданные криптоалгоритмы	16	16
Подготовка к экзамену	13,5	13.5
Подготовка к практическим занятиям. Выполнение домашних заданий	40	40
Консультации и промежуточная аттестация	10,5	10,5
Вид контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Введение в криптографию	4	2	2	0
2	Криптосистемы с секретным ключом	20	10	10	0
3	Криптосистемы с открытым ключом	22	10	12	0
4	Надежность шифров	4	4	0	0
5	Алгоритмы цифровой подписи	10	2	8	0
6	Современные стандарты шифрования	4	4	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
2	1	Исторический обзор. Открытые сообщения и их характери-стики. История криптографии. Примеры ручных шифров. Основные этапы становления	2

		криптографии как науки. Частотные характеристики открытых текстов. Основные задачи и понятия криптографииПеречень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели шифров. Основные требования к шифрам. Простейшие криптографические протоколы.	
4	2	Поточные шифры замены Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, анализ шифра Виженера. Шифры перестановки Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы анализа шифров перестановки.	4
5	2	Шифры Хилла. Шифры на основе псевдослучайных последовательностей. Линейные рекуррентные последовательности (ЛРП) над полем. Свойства ЛРП максимального периода. Линейная сложность псевдослучайной последовательности. Алгоритм Берлекампа-Месси.	6
8	3	«Public key cryptography»: Принцип построения шифрсистем с открытым ключом. Протокол Диффи-Хеллмана. Шифрсистема на основе задачи об “укладке рюкзака”. Шифрсистема RSA. Шифрсистема Эль-Гамаля.	4
10	3	Шифрсистема Нидеррайтера. Криптосистемы на основе эллиптических кривых.	6
13	4	Основы теории К.Шеннона Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ.	4
16	5	Общие требования к цифровой подписи. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль-Гамаля. Стандарты цифровой подписи.	2
17	6	Современные блочные шифрсистемы. Сети Фейстеля. Криптоалгоритм DES. Криптоалгоритм RIJNDAEL. Криптоалгоритм ГОСТ-28147-89	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Шифры замены. Шифр Виженера. Перестановочные шифры. Шифры Хилла	2
2	2	Контрольная работа по симметричным криптосистемам	1
3	2	Шифры на основе линейных рекуррентных последовательностей. Сети Фейстеля.	6
4	2	Контрольная работа по теме "Линейные рекуррентные последовательности"	2
5	2	Контрольная работа по теме "Сети Фейстеля"	1
6	3	Криптосистема на основе задачи о рюкзаке. Криптосистема RSA	4
7	3	Криптосистема Эль-Гамаля. Эллиптические кривые. Шифрсистемы на основе эллиптических кривых	4
8	3	Контрольная работа по асимметричным системам шифрования.	2
9	3	Элементы криптографического анализа.	1
10	3	Контрольная работа по теме "Криптографический анализ"	1
11	5	Цифровая подпись Эль-Гамаля.	4
12	5	Цифровая подпись Фиата-Шамира. Цифровая подпись Шнорра.	2
13	5	Контрольная работа по теме "Цифровые подписи"	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Написание программ, реализующих заданные криптоалгоритмы	Литература из основного и дополнительного списка	7	16
Подготовка к экзамену	Литература из основного и дополнительного списка	7	13,5
Подготовка к практическим занятиям. Выполнение домашних заданий	Литература из основного и дополнительного списка	7	40

6. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	7	Текущий контроль	Контрольная работа "Симметричные системы шифрования"	1	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
2	7	Текущий контроль	Контрольная работа "Шифры на основе линейных рекурретных последовательностей"	2	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
3	7	Текущий контроль	Контрольная работа "Сети Фейстеля"	1	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок	экзамен

						1 балл - имеются намеки на решение	
4	7	Текущий контроль	Контрольная работа "Асимметричные системы шифрования"	1	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
5	7	Текущий контроль	Контрольная работа "Криптосистема Нидеррайтера"	1	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
6	7	Текущий контроль	Контрольная работа "Эллиптические кривые"	1	5	5 баллов - все задания решены 4 балла - решены все задания с мелкими недочетами 3 балла - в решении имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен
7	7	Текущий контроль	Выступление с докладом	1	2	1 балл - тема раскрыта не полностью 2 балла - тема раскрыта	экзамен
8	7	Проме-жуточная аттестация	Экзамен	-	5	5 баллов - все задания выполнены правильно 4 балла - задания выполнены с мелкими недочетами 3 балла - имеются значительные ошибки 2 бала - имеется большое количество существенных ошибок 1 балл - имеются намеки на решение	экзамен

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	Экзамен проводится в форме устного опроса. В аудитории, где проводится экзамен, должно одновременно присутствовать не более 6-8 студентов. Каждому студенту задается по одному вопросу или заданию из каждой темы, выносимой на экзамен. При неправильном ответе студенту могут быть заданы уточняющие или новые вопросы из этой темы. Тема считается освоенной, если студент смог ответить на 2 вопроса, заданных	В соответствии с пп. 2.5, 2.6 Положения

	по этой теме, и решить одну задачу.	

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ							
		1	2	3	4	5	6	7	8
ПК-6	Знает: принципы построения криптографических алгоритмов, криптографические стандарты, основные подходы к реализации криптографических средств защиты информации	+	+	+	+	+	+	+	+
ПК-6	Имеет практический опыт: решения задач, связанных с распределением ключевой информации, шифрованием чувствительной информации и цифровой подписью сообщений	+	+	+	+	+	+		+

Типовые контрольные задания по каждому мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Зюляркина Н.Д. Криптографические методы защиты информации. Методические указания по проведению практических занятий

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронно-библиотечная система издательства Лань	Глухов М.М. Введение в теоретико-числовые методы в криптографии. -- СПб. : Лань, 2011. — 400 с. http://e.lanbook.com/
2	Дополнительная литература	Электронно-библиотечная система издательства Лань	Голиков, А.М. Методы шифрования информации в сетях и системах радиосвязи. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 329 с. http://e.lanbook.com/
3	Основная литература	Электронно-библиотечная система издательства Лань	Рябко, Б.Я. Основы современной криптографии и стеганографии. [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 232 с. http://e.lanbook.com/

Перечень используемого программного обеспечения:

Нет

Перечень используемых профессиональных баз данных и информационных справочных систем:

Нет

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лабораторные занятия	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Практические занятия и семинары	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2