ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Институт естественных и точных наук

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: 01.10.2021

А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П2.06 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: 30.09.2021

А. А. Замышляева

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Ножкина Т. Г.
Пользователь: nozhkinatg
Дата подписания: 30.09.2021

Т. Г. Ножкина

СОГЛАСОВАНО

Руководитель образовательной программы
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: 01.10.2021

А. А. Замышляева

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, 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
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

Математические основы криптографии	Знает: алгебраические структуры, лежащие в основе современных криптографических систем Умеет: использовать математические методы при создании криптографических спецификаций Имеет практический опыт:

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
с применением дистанционных образовательных технологий	0	
Подготовка к экзамену	20	20
Подготовка доклада	20	20
Подготовка к контрольным работам	29,5	29.5
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	8	4	4	0
2	Криптосистемы с секретным ключом	20	10	10	0
3	Криптосистемы с открытым ключом	24	12	12	0
4	Современные стандарты шифрования	12	6	6	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1-2	1	Исторический обзор. Открытые сообщения и их характеристики. История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. Основные задачи и понятия криптографии Перечень угроз. Симметричное и асимметричное шифрование в задачах защиты информации. Шифры с открытым ключом и их использование. Классификация шифров. Модели	4

		шифров. Основные требования к шифрам.	
3-4	2	Шифры перестановки Разновидности шифров перестановки: маршрутные и геометрические перестановки. Элементы анализа шифров перестановки. 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.	4
5-6	2	Шифры Вермана, Блейхера, Хилла. Магические квадраты.	4
7	2	Методы анализа криптографических алгоритмов Подходы к анализу криптографических алгоритмов. Метод перебора. Корреляционный метод анализа поточных шифров. Линейный и дифференциальный методы анализа блочных шифров.	2
8-9	3	Принцип построения шифрсистем с открытым ключом. Шифрсистема на основе задачи об “укладке рюкзака”	4
10-11	3	Шифрсистема RSA. Шифрсистема Эль-Гамаля.	4
12-13	3	Шифрсистема Нидеррайтера. Схема разделения секрета.	4
14	4	Группы точек эллиптических кривых.	2
15-16	4	Криптосистемы и шифрование на основе эллиптических кривых	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1-2	1	Шифры замены. Шифр Цезаря. Перестановочные шифры.	4
3-4	2	Шифры перестановки. Поточные шифры замены. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, Шифр Виженера.	4
5-6	2	Шифры Хилла, Блейхера, Вернама. Магические квадраты.	4
7	2	Контрольная работа по симметричным криптосистемам	2
8	3	Криптосистема на основе задачи о рюкзаке	2
9	3	Криптосистема RSA.	2
10-11	3	Криптосистема Эль-Гамаля.	4
12	3	Схема разделения секрета	2
13	3	Контрольная работа по асимметричным системам шифрования.	2
14	4	Нахождение группы точек эллиптической кривой.	2
15-16	4	Криптосистема на основе эллиптических кривых	4

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
Подготовка к экзамену	ЭУМД. осн. лит. п. 3, п. 4. доп. лит. п. 2.	7	20
Подготовка доклада	ПУМД. доп. лит. п.1.	7	20

Подготовка к контрольным работам	ЭУМД. осн. лит. п. 3, п. 4. доп. лит. п. 2.	7	29,5

6. Текущий контроль успеваемости, промежуточная аттестация

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 1	30	5	Студент получает за каждое [1-5] верно выполненное задание 1 балл.	экзамен
2	7	Текущий контроль	Контрольная работа 2	30	8	Студент получает за каждый верно выполненный пункт 1 балл.	экзамен
3	7	Текущий контроль	Доклад	20	5	Подготовлен доклад - 1 балл; Подготовлена презентация - 1 балл; Оформление презентации соответствует ГОСТ - 1 балл; Тема раскрыта - 1 балл; Доклад вызвал интерес у аудитории - 1 балл.	экзамен
4	7	Текущий контроль	Активная познавательная деятельность	20	32	На каждом из 32 занятий студент может получить 2 балла: Студент задает вопросы по докладу - 1 балл; Студент правильно отвечает на вопросы по докладу - 1 балл. В противном случае баллы не начисляются.	экзамен
5	7	Проме-жуточная аттестация	Экзамен	1	8	Студент получает 1 балл за каждое верно выполненное задание.	экзамен

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	Экзамен является обязательным контрольным мероприятием промежуточной аттестации. Студент получает билет и в течение 90 минут решает предложенные ему задачи. При этом допускается использование ПК. После чего, сдаёт работу преподавателю. Преподаватель проверяет работу и озвучивает результат с учётом баллов за текущий контроль.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5

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	+	+			+	+

Фонды оценочных средств по каждому контрольному мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

1. Зуев, Ю. А. По океану дискретной математики : От перечислительной комбинаторики до современной криптографии Текст Т. 2 Графы. Алгоритмы. Коды, блок-схемы, шифры Ю. А. Зуев. - М.: URSS : ЛИБРОКОМ, 2012. - 363 с. ил.

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

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 разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Голиков, А.М. Методы шифрования информации в сетях и системах радиосвязи. [Электронный ресурс] — Электрон. дан. — М. : ТУСУР, 2012. — 329 с. — Режим доступа: http://e.lanbook.com/book/11380 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Свободный
2	Дополнительная литература	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. — Режим доступа: http://e.lanbook.com/book/63244 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Свободный
3	Основная	Аграновский, А.В. Практическая	Электронно-	Интернет /

	литература	криптография: алгоритмы и их программирование. [Электронный ресурс] / А.В. Аграновский, Р.А. Хади. — Электрон. дан. — М. : СОЛОН-Пресс, 2009. — 256 с. — Режим доступа: http://e.lanbook.com/book/13653 — Загл. с экрана.	библиотечная система издательства Лань	Свободный
4	Основная литература	Глухов, М.М. Введение в теоретико-числовые методы криптографии. [Электронный ресурс] / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — СПб. : Лань, 2011. — 400 с. — Режим доступа: http://e.lanbook.com/book/68466 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Свободный

Перечень используемого программного обеспечения:

1. -Deductor Academic(бессрочно)
2. Math Works-MATLAB (Simulink R2008a, SYMBOLIC MATH)(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. -Консультант Плюс(31.07.2017)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	336 (3б)	Проектор, компьютер, экран.
Практические занятия и семинары	327 (3б)	Компьютеры