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: 26.09.2021

А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.06 Основы защиты информации в ЭВМ
для направления 01.03.02 Прикладная математика и информатика
уровень Бакалавриат
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: 25.09.2021

А. А. Замышляева

Разработчик программы,
к.физ.-мат.н., доцент

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Елсаков С. М.
Пользователь: elsakovsm
Дата подписания: 25.09.2021

С. М. Елсаков

СОГЛАСОВАНО

Руководитель направления
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: 26.09.2021

А. А. Замышляева

Челябинск

1. Цели и задачи дисциплины

Получение основных представлений об использовании криптографических методов, основанных на базе алгебры и теории чисел, для защиты информации при дистанционной передаче электронных финансовых документов, и в платежных системах, использующих электронные деньги. В результате изучения дисциплины студенты должны владеть основными математическими понятиями курса; уметь решать типовые задачи, уметь использовать математический аппарат для решения теоретических и прикладных задач криптографии.

Краткое содержание дисциплины

Защита информации в компьютерных системах Классические шифры и основные понятия криптографии Современные симметричные криптосистемы Основы теории чисел Криптосистемы с открытым ключом

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-2 Способен применять основные алгоритмические и программные решения в области информационно-коммуникационных технологий, а также участвовать в их разработке	Знает: основные концепции и методы защиты информации в ЭВМ Умеет: использовать методы защиты информации при создании программных решений в области информационно-коммуникационных технологий Имеет практический опыт: использования различных средств защиты информации в ЭВМ

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	1.Ф.08 Программирование на языке Java, 1.Ф.03 Визуальное программирование

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

Нет

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 54,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах

		Номер семестра
		3
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	32	32
Самостоятельная работа (СРС)	53,75	53,75
с применением дистанционных образовательных технологий	0	
Подготовка к зачету	23,75	23.75
Подготовка отчетов по лабораторным работам	30	30
Консультации и промежуточная аттестация	6,25	6,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Защита информации в компьютерных системах	8	4	0	4
2	Классические шифры	6	2	0	4
3	Симметричные криптосистемы	16	4	0	12
4	Введение в теорию чисел	8	4	0	4
5	Эллиптическая криптография	10	2	0	8

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Общая характеристика средств и методов защиты информации в компьютерных системах	2
2	1	Основные принципы защиты информации	2
3	2	Криптостойкость. Стандартные атаки	1
3	2	Классические шифры	1
4	3	Группы в симметричных криптосистемах	2
5	3	Сеть Фейстеля. SP-сеть. Лавинный эффект	2
6	4	Арифметика целых чисел. НОД. Алгоритм Евклида.	1
6	4	Линейные диофантовы уравнения. Вычеты. Инверсии.	1
7	4	Линейное сравнение. Квадратичное сравнение. Символ Лежандра.	1
7	4	Простые числа. Функция Эйлера.	1
8	5	Эллиптическая криптография	2

5.2. Практические занятия, семинары

Не предусмотрены

5.3. Лабораторные работы

№ занятия	№ раздела	Наименование или краткое содержание лабораторной работы	Кол-во часов
1,2	1	Классические шифры и основные понятия	4
5	2	Множества с алгеб-раическими операциями	2
6	2	Методы генерации псевдослучайных последовательностей	2
3,4	3	Симметричные криптосистемы	4
7,8	3	Поиск коллизия хэш-функций	4
9,10	3	Изучение лавинного эффекта в симметричных алгоритмах шифрования	4
11,12	4	Криптосистемы с открытым ключом	4
13,14	5	Криптографические протоколы	4
15,16	5	Криптоанализ алгоритма на основе эллиптической кривой	4

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 зачету	http://e.lanbook.com/book/3032	3	23,75
Подготовка отчетов по лабораторным работам		3	30

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	3	Текущий контроль	ЛР1	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6.	зачет

						Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
2	3	Текущий контроль	ЛР2	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
3	3	Проме-жуточная аттестация	Зачет	1	120	Контрольное мероприятие промежуточной аттестации (зачетная работа) включает устный ответ на билет и проводятся во время зачета При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов. В билете два вопроса. Критерии оценивания выполнения зачетной работы: - ответ на один вопрос из билета без замечаний – 30 баллов; - ответ на один вопрос из билета с недочетами – 20 баллов; - ответ на один вопрос из билета с грубыми замечаниями– 10 баллов; - нет ответа на один вопрос из билета – 0 баллов; - ответ на один дополнительный вопрос без замечаний – 30 баллов; - ответ на один дополнительный вопрос с недочетами– 20 баллов; - ответ на один дополнительный вопрос с грубыми замечаниями – 10 баллов; - нет ответ на один дополнительный вопрос– 0 баллов; Максимальное количество баллов за промежуточную аттестацию – 120.	зачет
4	3	Текущий контроль	Семестровая работа	9	48	Защита семестровой работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей: - алгоритм шифрования корректен – 16	зачет

						баллов - выводы логичны и обоснованы – 16 баллов - оформление работы соответствует требованиям – 16 баллов Максимальное количество баллов – 48. Весовой коэффициент мероприятия – 9.	
5	3	Текущий контроль	ЛР3	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
6	3	Текущий контроль	ЛР4	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
7	3	Текущий контроль	ЛР5	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл	зачет

						- правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
8	3	Текущий контроль	ЛР6	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
10	3	Текущий контроль	ЛР7	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
11	3	Текущий контроль	ЛР8	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6.	зачет

						Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
12	3	Текущий контроль	ЛР9	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
13	3	Текущий контроль	ЛР10	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
14	3	Текущий контроль	ЛР11	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет

15	3	Текущий контроль	ЛР12	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
16	3	Текущий контроль	ЛР13	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
17	3	Текущий контроль	ЛР14	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса). Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу): - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	зачет
18	3	Бонус	Поиск опечаток	4	15	За каждую опечатку начисляется 3 балла, максимально 15 баллов. Весовой	зачет

						коэффициент мероприятия – 4.	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Прохождение контрольных мероприятий промежуточной аттестации не обязательно. Зачет проводится по билетам. В билете два вопроса. Билет выбирается случайным образом. Студенту дается 30 минут на подготовку. После этого он рассказывает ответы на вопросы билета. Студенту задается дополнительный вопрос по каждому вопросу.	В соответствии с пп. 2.5, 2.6 Положения

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ															
		1	2	3	4	5	6	7	8	10	11	12	13	14	15	16	17	18
ПК-2	Знает: основные концепции и методы защиты информации в ЭВМ	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-2	Умеет: использовать методы защиты информации при создании программных решений в области информационно-коммуникационных технологий	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-2	Имеет практический опыт: использования различных средств защиты информации в ЭВМ	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

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:

Не предусмотрена

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

1. Конфидент

г) методические указания для студентов по освоению дисциплины:

1. Коробейников, А. Г. Математические основы криптографии. Учебное пособие / А. Г. Коробейников. – СПб: СПб ГУ ИТМО, 2002. – 41 с

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид	Наименование разработки	Наименование	Доступность

	литературы		ресурса в электронной форме	(сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Основная литература	Сергеева, Ю.С. Защита информации. Конспект лекций. [Электронный ресурс] — Электрон. дан. — М. : А-Приор, 2011. — 128 с. — Режим доступа: http://e.lanbook.com/book/3083 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
2	Дополнительная литература	Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с. — Режим доступа: http://e.lanbook.com/book/3032 — Загл. с экрана.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. -MinIDE (сборка из SciTE, MinGW C/C++, GDB)(бессрочно)

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	333 (3б)	Компьютеры с ОС Windows и доступом в Internet
Лекции	333 (3б)	Доска с фломастерами