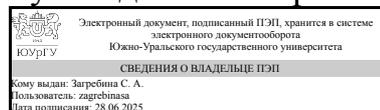


УТВЕРЖДАЮ:
Руководитель направления



С. А. Загребина

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.22 Основы компьютерной безопасности
для направления 02.03.02 Фундаментальная информатика и информационные технологии

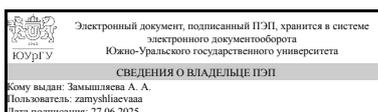
уровень Бакалавриат

форма обучения очная

кафедра-разработчик Прикладная математика и программирование

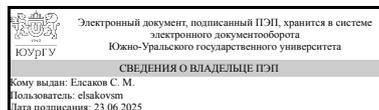
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии, утверждённым приказом Минобрнауки от 23.08.2017 № 808

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



А. А. Замышляева

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



С. М. Елсаков

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
ОПК-3 Способен к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям	Знает: основные концепции компьютерной безопасности и методы защиты информации в области информационно-коммуникационных технологий Умеет: использовать методы защиты информации при создании программных решений в области информационно-коммуникационных технологий
ОПК-5 Способен устанавливать и сопровождать программное обеспечение информационных систем и баз данных, в том числе отечественного происхождения, с учетом информационной безопасности	Умеет: использовать современное ПО с учетом информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.16 Методы программирования	Не предусмотрены

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

Дисциплина	Требования
1.О.16 Методы программирования	Знает: принципы представление данных в памяти компьютера, порядок работы операторов языка программирования Умеет: выполнять разработку и отладку программ на языках

	программирования высокого уровня Имеет практический опыт: работы с различными системами программирования, различными средами программирования
--	---

4. Объём и виды учебной работы

Общая трудоёмкость дисциплины составляет 3 з.е., 108 ч., 72,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		3	
Общая трудоёмкость дисциплины	108	108	
<i>Аудиторные занятия:</i>	64	64	
Лекции (Л)	32	32	
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32	
Лабораторные работы (ЛР)	0	0	
<i>Самостоятельная работа (СРС)</i>	35,5	35,5	
Подготовка к зачету	35,5	35,5	
Консультации и промежуточная аттестация	8,5	8,5	
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	Защита информации в компьютерных системах	8	4	4	0
2	Классические шифры	10	6	4	0
3	Симметричные криптосистемы	14	6	8	0
4	Введение в теорию чисел	22	14	8	0
5	Эллиптическая криптография	10	2	8	0

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	Классические шифры	4
3	2	Криптостойкость. Стандартные атаки	2
4	3	Группы в симметричных криптосистемах	4
5	3	Сеть Фейстеля. SP-сеть. Лавинный эффект	2

6	4	Арифметика целых чисел. НОД. Алгоритм Евклида.	4
6	4	Линейные диофантовы уравнения. Вычеты. Инверсии.	4
7	4	Линейное сравнение. Квадратичное сравнение. Символ Лежандра.	2
7	4	Простые числа. Функция Эйлера.	4
8	5	Эллиптическая криптография	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1,2	1	Классические шифры и основные понятия	4
5	2	Множества с алгебраическими операциями	2
6	2	Методы генерации псевдослучайных последовательностей	2
3, 4	3	Симметричные криптосистемы	4
9,10	3	Изучение лавинного эффекта в симметричных алгоритмах шифрования	4
7,8	4	Поиск коллизия хэш-функций	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

5.3. 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 зачету	http://e.lanbook.com/book/3032	3	35,5

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-мestr	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учитывается 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).	экзамен

						<p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. <p>Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.</p>	
2	3	Текущий контроль	ЛР2	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. <p>Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.</p>	экзамен
3	3	Промежуточная аттестация	Зачет	-	120	<p>Контрольное мероприятие промежуточной аттестации (зачетная работа) включает устный ответ на билет и проводятся во время зачета</p> <p>При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов. В билете два вопроса.</p> <p>Критерии оценивания выполнения зачетной работы:</p> <ul style="list-style-type: none"> - 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; 	экзамен

						<p>- нет ответ на один дополнительный вопрос – 0 баллов; Максимальное количество баллов за промежуточную аттестацию – 120.</p>	
4	3	Текущий контроль	Семестровая работа	9	48	<p>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 баллов - выводы логичны и обоснованы – 16 баллов - оформление работы соответствует требованиям – 16 баллов Максимальное количество баллов – 48. Весовой коэффициент мероприятия – 9.</p>	экзамен
5	3	Текущий контроль	ЛР3	1	6	<p>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.</p>	экзамен
6	3	Текущий контроль	ЛР4	1	6	<p>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.</p>	экзамен

						Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
7	3	Текущий контроль	ЛР5	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. <p>Максимальное количество баллов – 6.</p> <p>Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.</p>	экзамен
8	3	Текущий контроль	ЛР6	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. <p>Максимальное количество баллов – 6.</p> <p>Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.</p>	экзамен
10	3	Текущий контроль	ЛР7	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. 	экзамен

						Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
11	3	Текущий контроль	ЛР8	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. <p>Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.</p>	экзамен
12	3	Текущий контроль	ЛР9	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. <p>Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.</p>	экзамен
13	3	Текущий контроль	ЛР10	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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 	экзамен

						балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
14	3	Текущий контроль	ЛР11	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. <p>Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.</p>	экзамен
15	3	Текущий контроль	ЛР12	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - 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. <p>Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.</p>	экзамен
16	3	Текущий контроль	ЛР13	1	6	<p>Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается качество оформления, правильность выводов и ответы на вопросы (задается 1 вопроса).</p> <p>Общий балл при оценке складывается из следующих показателей (за каждую лабораторную работу):</p> <ul style="list-style-type: none"> - приведены методики оценки технологических параметров – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл 	экзамен

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:

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 литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	ЭБС издательства Лань	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.
2	Дополнительная литература	ЭБС издательства Лань	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.

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	333	Компьютеры с ОС Windows и доступом в Internet

занятия	(3б)	
Лекции	333 (3б)	Доска с фломастерами