ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 14.08.2023

А. А. Замышляева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.19 Основы защиты данных в интеллектуальных системах
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.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Замышляева А. А.
Пользователь: zamyshliaevaaa
Дата подписания: 14.08.2023

А. А. Замышляева

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

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Елсаков С. М.
Пользователь: elsakovsm
Дата подписания: 08.08.2023

С. М. Елсаков

Челябинск

1. Цели и задачи дисциплины

Получение основных представлений об использовании криптографических методов, основанных на базе алгебры и теории чисел, для защиты данных в интеллектуальных системах. 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. Уметь организовывать защиту данных в интеллектуальных системах.

Краткое содержание дисциплины

Основные термины. Основы организации защиты данных в интеллектуальных системах. Классические шифры и основные понятия криптографии. Современные симметричные криптосистемы. Криптосистемы с открытым ключом. Основы теории чисел и эллиптические кривые.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
УК-11 Способен планировать и организовывать свою деятельность в цифровом пространстве с учётом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности.	Знает: [УК-1.2. З-1.] цели задачи и предмет, основные понятия информационной безопасности, информационные угрозы, их классификацию, возможные последствия для организаций различных форм собственности и критерии оценки защищённости информационных систем и систем искусственного интеллекта Умеет: [УК-1.2. У-2.] сознавать опасности и угрозы, возникающие в профессиональной деятельности и в социальной сфере, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны; [УК-1.2. У-3.] работать с информацией с учётом требований информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	1.О.35 Современные технологии разработки программных систем искусственного интеллекта, 1.О.36 Анализ требований и проектирование систем искусственного интеллекта, Производственная практика (технологическая, проектно-технологическая) (6 семестр)

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., 70,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		4
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	0	0
Лабораторные работы (ЛР)	32	32
Самостоятельная работа (СРС)	37,5	37,5
Выполнение семестровой работы	20	20
Подготовка к зачету	17,5	17.5
Консультации и промежуточная аттестация	6,5	6,5
Вид контроля (зачет, диф.зачет, экзамен)	-	диф.зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Организация защиты данных в интеллектуальных системах	14	6	0	8
2	Классические шифры	14	4	0	10
3	Симметричные криптосистемы	10	6	0	4
4	Введение в теорию чисел	24	14	0	10
5	Эллиптическая криптография	2	2	0	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Общая характеристика средств и методов защиты данных в интеллектуальных системах	2
2	1	Основные принципы и модели защиты информации	4
3	2	Криптостойкость. Стандартные атаки	2
3	2	Классические шифры	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	Простые числа. Функция Эйлера.	4
7	4	Линейное сравнение. Квадратичное сравнение. Символ Лежандра.	2
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
5	1	Стеганография	2
6	1	Псевдослучайные последовательности	2
8	1	Коллизии хэш-функций	2
11	1	Программные средства криптографии	2
1	2	Моноалфавитные шифры	4
2	2	Полиалфавитные шифры	4
7	2	Изучение лавинного эффекта в симметричных алгоритмах шифрования	2
3	3	Метод вероятных слов	2
4	3	Полный перебор	2
9	4	Простые числа	2
10	4	Символы Лежандра	2
12	4	RSA	2
13	4	Дискретное логарифмирование	2
14	4	Алгоритм Рабина	2

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Выполнение семестровой работы	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.	4	20
Подготовка к зачету	Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. — Москва : ДМК Пресс, 2012. — 592 с. — ISBN 978-5-94074-637-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/3032 (дата обращения: 06.08.2023). — Режим	4	17,5

	доступа: для авториз. пользователей.		

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	4	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. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	дифференцированный зачет
2	4	Текущий	ЛР2	1	6	Защита лабораторной	дифференцированный

		контроль				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	4	Проме-жуточная аттестация	Дифференцированный зачет	-	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	дифференцированный зачет

						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.	
4	4	Текущий контроль	Семестровая работа	1	15	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	дифференцированный зачет

						шифрования корректен – 5 баллов - выводы логичны и обоснованы – 5 баллов - оформление работы соответствует требованиям – 5 баллов Максимальное количество баллов – 15. Весовой коэффициент мероприятия – 1.	
5	4	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.	дифференцированный зачет
6	4	Текущий контроль	ЛР4	1	6	Защита лабораторной работы	дифференцированный зачет

						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.	
7	4	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	дифференцированный зачет

						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.	
8	4	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 –	дифференцированный зачет

						6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
9	4	Текущий контроль	Тест по определениям	1	9	Тест проводится в системе Электронный ЮУрГУ на выделенном занятии. Общий балл при оценке складывается из ответов на 9 вопросов: - верно сопоставлено определение и понятие – 1 балл (за каждый вопрос); Максимальное количество баллов – 9. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	дифференцированный зачет
10	4	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	дифференцированный зачет

						один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
11	4	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. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	дифференцированный зачет
12	4	Текущий контроль	ЛР9	1	6	Защита лабораторной работы осуществляется индивидуально. Студентом предоставляется	дифференцированный зачет

						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.	
13	4	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	дифференцированный зачет

						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.	
14	4	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	дифференцированный зачет

						лабораторную работу) – 1.	
15	4	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.	дифференцированный зачет
16	4	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	дифференцированный зачет

						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.	
17	4	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	дифференцированный зачет

						один вопрос – 3 балла. Максимальное количество баллов – 6. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	
18	4	Бонус	Поиск опечаток	-	15	За каждую опечатку начисляется 3 балла, максимально 15 баллов. Весовой коэффициент мероприятия – 4.	дифференцированный зачет
19	4	Текущий контроль	Контрольная	1	20	Контрольная проводится в системе Электронный ЮУрГУ на выделенном занятии. Общий балл при оценке складывается из следующих показателей: - верно решена задача на быстрое возведение в степень – 1 балл; - верно решена задача на формулу Эйлера – 1 балл; - верно решена задача на линейное сравнение – 2 балла; - верно решена задача на систему линейных сравнений - 3 балла; - верно решена задача на квадратичное сравнение - 2 балла; - верно решена задача на первообразные корни - 2 балла; - верно решена задача дискретного логарифмирования - 2 балла; - верно решена задача принадлежности точки эллиптической кривой - 1 балл; - верно решена задача суммы точек на эллиптической кривой - 6 баллов;	дифференцированный зачет

						Максимальное количество баллов – 20. Весовой коэффициент мероприятия (за каждую лабораторную работу) – 1.	

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
дифференцированный 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. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
УК-11	Знает: [УК-1.2. З-1.] цели задачи и предмет, основные понятия информационной безопасности, информационные угрозы, их классификацию, возможные последствия для организаций различных форм собственности и критерии оценки защищённости информационных систем и систем искусственного интеллекта	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
УК-11	Умеет: [УК-1.2. У-2.] сознавать опасности и угрозы, возникающие в профессиональной деятельности и в социальной сфере, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны; [УК-1.2. У-3.] работать с информацией с учётом требований информационной безопасности	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

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	Электронно-библиотечная система 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	Электронно-библиотечная система 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. LibreOffice(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
Лекции	333 (3б)	Доска с фломастерами
Лабораторные занятия	333 (3б)	Компьютеры с ОС Windows и доступом в Internet