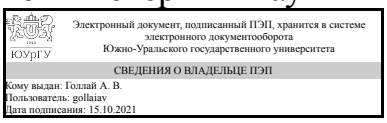
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук



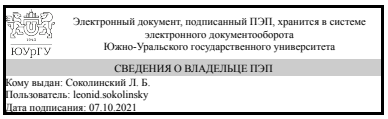
А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.03 Криптография и защита информации
для направления 02.04.02 Фундаментальная информатика и информационные технологии
уровень Магистратура
форма обучения очная
кафедра-разработчик Системное программирование

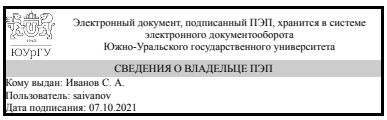
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 02.04.02 Фундаментальная информатика и информационные технологии, утверждённым приказом Минобрнауки от 23.08.2017 № 811

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



Л. Б. Соколинский

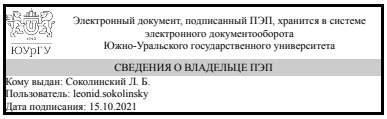
Разработчик программы,
к.физ.-мат.н., доцент (кн)



С. А. Иванов

СОГЛАСОВАНО

Руководитель направления
д.физ.-мат.н., проф.



Л. Б. Соколинский

Челябинск

1. Цели и задачи дисциплины

Предметом дисциплины являются основные понятия безопасности информационных технологий. Целью дисциплины является изучение основных концепций в сфере информационной безопасности и практическое освоение математических методов и алгоритмов защиты информации. Основные задачи дисциплины: ознакомить студента с математическими основами информационной безопасности, математическими методами, моделями и алгоритмами защиты информации.

Краткое содержание дисциплины

1) Основные понятия информационной безопасности 2) Кодирование как инструмент безопасной работы с информацией 3) Основные понятия и задачи криптографии 4) Теоретические основы компьютерной безопасности

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ОПК-3 Способен проводить анализ математических моделей, создавать инновационные методы решения прикладных задач профессиональной деятельности в области информатики и математического моделирования	Знает: основные подходы к математической формализации различных аспектов безопасности информационных систем и реализации средств защиты информации Умеет: применять математические методы и алгоритмы защиты информации при решении профессиональных задач в области информационной безопасности Имеет практический опыт: самостоятельного формулирования задач и политик безопасности, построения систем защиты
ОПК-4 Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	Знает: основные требования информационной безопасности, основные алгоритмы шифрования данных, базовые понятия для математического обеспечения информационной безопасности Умеет: применять математические методы защиты информации, кодировать информацию с помощью основных алгоритмов шифрования Имеет практический опыт: кодирования информации основными алгоритмами шифрования, реализованными на языке высокого уровня

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	1.О.19 Разработка игр для социальных сетей, 1.О.08 Анализ информационных технологий, 1.О.13 Интеллектуальный анализ данных, 1.О.07 Современные технологии разработки ПО, 1.О.06 Объектно-ориентированные CASE-

	технологии, 1.О.05 Архитектура распределенных программных систем, 1.О.10 Нейронные сети

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., 56,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		1
Общая трудоёмкость дисциплины	108	108
Аудиторные занятия:	48	48
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	51,5	51,5
с применением дистанционных образовательных технологий	0	
Изучение дополнительного материала по основам теории чисел.	21,5	21.5
Подготовка к экзамену	10	10
Изучение дополнительного материала по шифрам с открытыми ключами, цифровой подписи и криптографии на эллиптических кривых.	20	20
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	Основные понятия информационной безопасности	12	10	2	0
2	Теория информации. Кодирование	12	8	4	0
3	Основные понятия и задачи криптографии	10	6	4	0
4	Теоретические основы компьютерной безопасности	8	4	4	0
5	Модели информационной безопасности	6	4	2	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие конфиденциальности, целостности, доступности информации. Модели безопасности. Понятие информационной безопасности. Гарантии обеспечения уровня информационной безопасности.	4
2	1	Понятие компьютерной атаки, типы атак. Понятие уязвимости и угрозы в информационной безопасности.	2
3	1	Составляющие информационной безопасности, основные методы обеспечения информационной безопасности, понятие защиты в глубину.	4
4	2	Математический подход к информации и кодированию.	4
5	2	Линейные коды. Нахождение ошибок. Исправление ошибок. Известные и популярные коды.	4
6	3	Краткий исторический обзор развития криптографии. Формальное определение шифра. Симметрические и асимметрические шифры.	2
7	3	Стандарт шифрования DES. Криптосистема RSA. Криптографические протоколы. Электронные цифровые подписи (ЭЦП). Криптографические средства и методы защиты данных программного обеспечения.	4
8	4	Компьютерная система (КС), информация, доступ, защищённость, безопасность. Политика безопасности. Формализация. Определения источника, потока информации, доступа, легальных и несанкционированных потоков, правил доступа.	4
9	5	Модели информационной безопасности CIA и Parkerian hexad	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие конфиденциальности, целостности, доступности информации.	2
2	2	Математический подход к информации и кодированию.	2
3	2	Линейные коды. Реализация простейшего кодирования и декодирования.	2
4	3	Электронные цифровые подписи (ЭЦП). Криптографические средства и методы защиты данных программного обеспечения.	2
5	3	Контроль целостности программного обеспечения.	2
6	4	Компьютерная система (КС), информация, доступ, защищённость, безопасность. Политика безопасности. Защита носителей информации.	2
7	4	Идентификация и аутентификация. Парольные системы защиты. Системы криптографической защиты информации.	2
8	5	Модели информационной безопасности	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	Семестр	Кол-во

	ресурс		часов
Изучение дополнительного материала по основам теории чисел.	Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система.	1	21,5
Подготовка к экзамену	Основная литература 1-3, дополнительная литература 1-2	1	10
Изучение дополнительного материала по шифрам с открытыми ключами, цифровой подписи и криптографии на эллиптических кривых.	Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Лань : электронно-библиотечная система.	1	20

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	1	Текущий контроль	Математический подход к информации и кодированию.	5	5	5 баллов: полностью выполнено практическое задание, даны правильные ответы на контрольные вопросы. 1-4 балла: задание выполнено частично или выполнено с ошибками, которые были исправлены студентом через некоторое время (2 попытка сдачи работы) 0 баллов: задание не выполнено	экзамен
2	1	Текущий контроль	Линейные коды. Реализация простейшего кодирования и декодирования.	5	5	5 баллов: полностью выполнено практическое задание, даны правильные ответы на контрольные вопросы. 1-4 балла: задание выполнено частично или выполнено с ошибками, которые были исправлены студентом через некоторое время (2 попытка сдачи работы) 0 баллов: задание не выполнено	экзамен
3	1	Текущий контроль	Компьютерная система (КС), информация, доступ,	5	5	5 баллов: полностью выполнено практическое задание, даны правильные ответы на контрольные	экзамен

			защищённость, безопасность. Политика безопасности. Защита носителей информации.			вопросы. 1-4 балла: задание выполнено частично или выполнено с ошибками, которые были исправлены студентом через некоторое время (2 попытка сдачи работы) 0 баллов: задание не выполнено	
4	1	Текущий контроль	Идентификация и аутентификация. Парольные системы защиты. Системы криптографической защиты информации.	5	5	5 баллов: полностью выполнено практическое задание, даны правильные ответы на контрольные вопросы. 1-4 балла: задание выполнено частично или выполнено с ошибками, которые были исправлены студентом через некоторое время (2 попытка сдачи работы) 0 баллов: задание не выполнено	экзамен
5	1	Проме-жуточная аттестация	Итоговый тест	30	30	Компьютерный тест состоит из 30 вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 1 час. Стоимость одного вопроса - 1 балл. 30 баллов: задание полностью выполнено без ошибок 1-29 баллов: задание выполнено частично или выполнено с ошибками 0 баллов: задание не выполнено	экзамен

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	На экзамене происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Отлично: Величина рейтинга обучающегося по дисциплине 85…100 % Хорошо: Величина рейтинга обучающегося по дисциплине 75…84 % Удовлетворительно: Величина рейтинга обучающегося по дисциплине 60…74 % Неудовлетворительно: Величина рейтинга обучающегося по дисциплине 0…59 %. Допускается выставление оценки на основе текущего рейтинга (автоматом).	В соответствии с пп. 2.5, 2.6 Положения

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5

ОПК-3	Знает: основные подходы к математической формализации различных аспектов безопасности информационных систем и реализации средств защиты информации	+	+	+	+	+	
ОПК-3	Умеет: применять математические методы и алгоритмы защиты информации при решении профессиональных задач в области информационной безопасности	+	+	+	+	+	
ОПК-3	Имеет практический опыт: самостоятельного формулирования задач и политик безопасности, построения систем защиты	+		+	+	+	
ОПК-4	Знает: основные требования информационной безопасности, основные алгоритмы шифрования данных, базовые понятия для математического обеспечения информационной безопасности	+	+	+	+	+	
ОПК-4	Умеет: применять математические методы защиты информации, кодировать информацию с помощью основных алгоритмов шифрования	+	+			+	+
ОПК-4	Имеет практический опыт: кодирования информации основными алгоритмами шифрования, реализованными на языке высокого уровня	+	+			+	+

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:

Не предусмотрены

г) методические указания для студентов по освоению дисциплины:

1. Методическое пособие

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	Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/165837
2	Основная литература	Электронно-библиотечная система издательства Лань	Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/111097

3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Котов, Ю. А. Криптографические методы защиты информации. Стандартные шифры. Шифры с открытым ключом : учебное пособие / Ю. А. Котов. — Новосибирск : НГТУ, 2017. — 67 с. — ISBN 978-5-7782-3411-6. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/118230
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/140740
5	Основная литература	Электронно-библиотечная система издательства Лань	Березкин, Е. Ф. Основы теории информации и кодирования : учебное пособие / Е. Ф. Березкин. — 3-е изд., стер. — Санкт-Петербург : Лань, 2019. — 320 с. — ISBN 978-5-8114-4119-8. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/115524

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
Экзамен	110 (3г)	Компьютеры, проектор
Лекции	110 (3г)	Компьютеры, проектор, доска
Практические занятия и семинары	110 (3г)	Компьютеры, проектор, доска