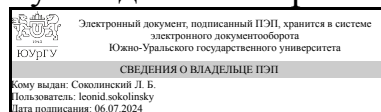


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления



Л. Б. Соколинский

РАБОЧАЯ ПРОГРАММА

дисциплины 1.О.03 Криптография и защита информации
для направления 02.04.02 Фундаментальная информатика и информационные технологии

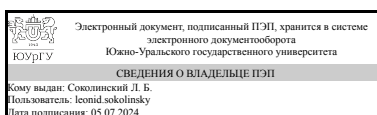
уровень Магистратура

форма обучения очная

кафедра-разработчик Системное программирование

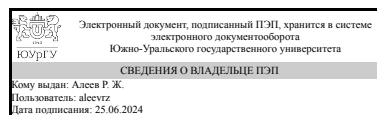
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 02.04.02 Фундаментальная информатика и информационные технологии, утверждённым приказом Минобрнауки от 23.08.2017 № 811

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



Л. Б. Соколинский

Разработчик программы,
д.физ.-мат.н., доц., профессор



Р. Ж. Алеев

1. Цели и задачи дисциплины

Предметом дисциплины "Криптография и защита информации" 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 криптографии и защиты информации.

Краткое содержание дисциплины

1) Математические понятия и результаты, используемые в криптографии и защите информации 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: использования основных алгоритмов шифрования для защиты данных и информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Нет	1.О.20 Интеллектуальный анализ данных, 1.О.04 Архитектура распределенных вычислительных систем, 1.О.15 Введение в Индустрию 4.0, 1.О.07 Анализ информационных технологий,

1.О.16 Квантовые вычисления,
1.О.06 Современные методы DevOps,
1.О.19 Компьютерное зрение

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 2 з.е., 72 ч., 36,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		1
Общая трудоёмкость дисциплины	72	72
<i>Аудиторные занятия:</i>	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	35,75	35,75
Доклады. Примерные темы 1) Применение сравнений в вычислениях 2) Анонимность в сети, 3) Квантовая передача информации, 4) Документы по информационной безопасности, 5) Нелинейные коды. Недвоичные коды, 6) Шифры на эллиптических кривых	17,75	17,75
Освоение различных математических пакетов	10	10
Изучение теоретико- числовых методов в криптографии	4	4
Решение задач по теории чисел.	4	4
Консультации и промежуточная аттестация	4,25	4,25
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	Математические понятия и результаты, используемые в криптографии и защите информации	8	4	4	0
2	Кодирование как инструмент безопасной работы с информацией	8	4	4	0
3	Основные понятия и задачи криптографии	8	4	4	0
4	Основные понятия и задачи криптографии	8	4	4	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Простые числа. Основная теорема арифметики. Число простых в интервале. Факторизация больших чисел. Сравнения. Случай простого модуля. Первообразный корень. Дискретный логарифм	2
2	1	Группы. Симметрическая группа. Кольцо, поле. Конечные поля и их строение	2
3	2	Математический подход к информации и кодированию	2
4	2	Линейные коды. Нахождение ошибок. Исправление ошибок. Известные и популярные коды. Новые подходы к кодам	2
5	3	Краткий исторический обзор развития криптографии. Формальное определение шифра. Симметрические и асимметрические шифры. Требования безопасности для шифрования	2
6	3	Стандарт шифрования ГОСТ 28147-89. Обоснование криптосистемы RSA. Протокол открытого распределения ключей Диффи-Хеллмана. Хэширование. Электронные цифровые подписи (ЭЦП).	2
7	4	Компьютерная система (КС), информация, доступ, защищённость, безопасность. Политика безопасности. Формализация. Аксиомы защищённых КС. Описание безопасности в КС (достоверность, доступность, целостность, конфиденциальность, актуальность). Угрозы КС. Определения источника, ассоциированности, потока информации, доступа, легальных и несанкционированных потоков, правил доступа	2
8	4	Модели Take-Grant, Белла-Лападуллы и др. Изолированная программная среда. Защита носителей информации. Идентификация и аутентификация. Парольные системы защиты. Системы криптографической защиты информации. Целостность в КС по Кларку и Вилсону. Документы по безопасности	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Основные методы работы с целыми числами в криптографии и защите информации	2
2	1	Алгебраические методы для работы с информацией	2
3	2	Математические вопросы теории информации	2
4	2	Построение линейных кодов	2
5	3	Построение и анализ шифров	2
6	3	Система RSA	2
7	4	Основные понятия компьютерных систем и их значение для защиты информации	2
8	4	Модели компьютерной 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 ресурс	Семестр	Кол-во часов
Доклады. Примерные темы 1) Применение сравнений в вычислениях 2) Анонимность в сети, 3) Квантовая передача информации, 4) Документы по информационной безопасности, 5) Нелинейные коды. Недвоичные коды, 6) Шифры на эллиптических кривых	1) Виноградов И.М.. Основы теории чисел. М: Лань, 2009, 2) и 3) Сведения из Интернета, 4) Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. М: Горячая линия - Телеком, 2006, 5) Мак-Вильямс Ф.Дж., Слоэн Н. Дж.А. Теория кодов, исправляющих ошибки. М.: Связь, 1979, 6) Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2006	1	17,75
Освоение различных математических пакетов	Документация по GAP https://www.gap-system.org/ Maple, Mathematica Matlab https://www.matburo.ru/st_subject.php?p=math	1	10
Изучение теоретико-числовых методов в криптографии	Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2006 Главы 1-5	1	4
Решение задач по теории чисел.	Виноградов И.М.. Основы теории чисел. М: Лань, 2009 Главы 3,4,6	1	4

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	Учитывается в ПА
1	1	Текущий контроль	Математические понятия и результаты, используемые в информационной безопасности	1	15	Данный вид контроля проводится в виде теста, в котором 3 задания. Каждое задание оценивается в 5 баллов. При неполном выполнении задания количество баллов снижается.	зачет
2	1	Текущий контроль	Теория информации. Кодирование	1	15	Данный вид контроля проводится в виде теста, в котором 3 задания. Каждое задание оценивается в 5 баллов. При неполном выполнении задания количество баллов снижается.	зачет
3	1	Текущий контроль	Основные понятия и задачи криптографии	1	15	Данный вид контроля проводится в виде теста, в котором 3 задания. Каждое задание оценивается в 5 баллов. При неполном выполнении задания количество баллов снижается.	зачет

4	1	Текущий контроль	Теоретические основы компьютерной безопасности	1	10	Данный вид контроля проводится в виде теста, в котором 2 задания. Каждое задание оценивается в 5 баллов. При неполном выполнении задания количество баллов снижается.	зачет
5	1	Бонус	Доклад	-	10	Тема доклада выбирается магистрантом по согласованию с преподавателем. Доклад делается на занятии и представляется в виде презентации. Также может быть представлен текст доклада. Доклад оценивается в 10 баллов. Снижение количества баллов допускается только в крайних случаях, когда доклад не удовлетворительно раскрывает заявленную тему.	зачет
6	1	Промежуточная аттестация	Финальный тест	-	48	Финальный тест проводится путём компьютерного тестирования. Финальный тест содержит 16 заданий. Каждое задание оценивается в 3 балла.	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (Положение о БРС утверждено приказом ректора от 24.05.2019 г. № 179, в редакции приказа ректора от 10.03.2022 г. No 25-13/09). Процедура прохождения промежуточной аттестации осуществляется согласно Положению о текущем контроле успеваемости и промежуточной аттестации (приказ ректора от 27.02.2024 № 33-13/09). Оценка за дисциплину формируется на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля: Зачтено: Величина рейтинга обучающегося по дисциплине 60...100 %. Незачтено: Величина рейтинга обучающегося по дисциплине 0...59 %. Если студент согласен с оценкой, полученной по результатам текущего контроля, то он может в день, предшествующий промежуточной аттестации дать свое согласие на автомат в личном кабинете. В случае явки студента на промежуточную аттестацию, давшего свое согласие на автомат в личном кабинете, студент имеет право пройти мероприятия текущего контроля по дисциплине на промежуточной аттестации для улучшения своего рейтинга в день ее проведения. Снижение оценки в этом случае запрещено. Если студент не дал согласия в личном кабинете, то он может согласиться с оценкой лично на промежуточной аттестации в день ее проведения. Если студент не согласен с оценкой, то он имеет право пройти контрольно-рейтинговые мероприятия на промежуточной аттестации для улучшения своего рейтинга в день ее проведения. Фиксация результатов учебной деятельности по	В соответствии с пп. 2.5, 2.6 Положения

	дисциплине проводится в день промежуточной аттестации на основе согласия студента, данного им в личном кабинете. При отсутствии согласия в журнале дисциплины фиксация результатов происходит при личном присутствии студента. Если студент не дал согласие в личном кабинете и не явился на промежуточную аттестацию – ему выставляется «неявка». Промежуточная аттестация проводится в форме тестирования. Тестирование проводится в системе edu.susu.ru. Тест содержит 16 вопросов. На выполнение теста дается 60 минут. В этом случае оценка за дисциплину рассчитывается на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации.	
--	---	--

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ					
		1	2	3	4	5	6
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: использования основных алгоритмов шифрования для защиты данных и 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:

1. Мельников, В. П. Защита информации [Текст] учебник для вузов по направлению 230100 "Информатика и вычисл. техника" (бакалавриат) В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - М.: Академия, 2014. - 296 с. ил.
2. Мельников, В. П. Информационная безопасность и защита информации [Текст] учеб. пособие В. П. Мельников и др.; под ред. С. А. Клейменова. - 4-е изд., стер. - М.: Академия, 2009. - 330, [1] с.

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

1. 1. Вестник УрФО. Безопасность в информационной сфере

г) методические указания для студентов по освоению дисциплины:

1. Алеев, Р. Ж. Математические основы защиты информации и информационной безопасности [Текст] учеб. пособие для магистрантов

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Алеев, Р. Ж. Математические основы защиты информации и информационной безопасности [Текст] учеб. пособие для магистрантов

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	Электронный архив ЮУрГУ	Алеев, Р. Ж. Математические основы защиты информации и информационной безопасности [Текст] учеб. пособие для магистрантов Р. Ж. Алеев ; Юж.-Урал. гос. ун-т, Высш. шк. электроники и компьютер. наук ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2017. - 125, [1] с. ил. электрон. версия. — Текст : электронный // Электронный архив ЮУрГУ — URL: https://dspace.susu.ru/xmlui/ (дата обращения: 20.09.2021). — Режим доступа: для авториз. пользователей. https://dspace.susu.ru/xmlui/
2	Основная литература	Электронно-библиотечная система издательства Лань	Краковский Ю. М. Методы защиты информации Издательство "Лань" — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 30.09.2021). — Режим доступа: для авториз. пользователей.
3	Основная литература	Электронно-библиотечная система издательства Лань	Бондарев Е. С., Васюков В. М., Грушевский П. Р., Скулябина О. В. Защита компьютерной информации: Учебное пособие Балтийский государственный технический университет «Военмех» имени Д.Ф. Устинова — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157086 (дата обращения: 30.09.2021). — Режим доступа: для авториз. пользователей.
4	Основная литература	Электронно-библиотечная система издательства Лань	Ярочкин В. И. Информационная безопасность: Учебник для вузов Издательство «Академический Проект» — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242 (дата обращения: 30.09.2021). — Режим доступа: для авториз. пользователей.
5	Основная литература	Электронно-библиотечная система издательства Лань	Коржик В. И., Яковлев В. А. Основы криптографии: Учебное пособие для обучающихся по направлениям подготовки бакалавров и магистров: 10.04.01, 10.03.01 «Информационная безопасность», 43.03.01 «Сервис», 11.03.02, 11.04.02 «Инфокоммуникационные технологии и системы связи», а также по специальности 210403 «Защищенные системы связи» ИЦ Интермедия — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161359 (дата обращения: 30.09.2021). — Режим доступа: для авториз. пользователей.

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
Практические занятия и семинары	110 (3г)	Проектор, MS Office, Adobe Reader для PDF
Лекции	110 (3г)	Проектор, MS Office, Adobe Reader для PDF