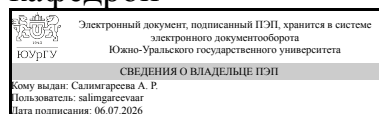


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Заведующий выпускающей
кафедрой



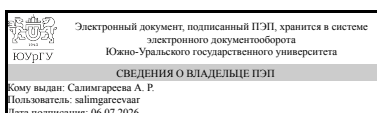
А. Р. Салимгареева

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П0.03 Основы информационной безопасности
для направления 09.03.04 Программная инженерия
уровень Бакалавриат
профиль подготовки Разработка информационных систем
форма обучения очная
кафедра-разработчик Гуманитарные, естественно-научные и технические дисциплины

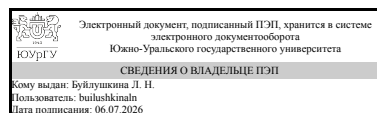
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.04 Программная инженерия, утверждённым приказом Минобрнауки от 19.09.2017 № 920

Зав.кафедрой разработчика,
к.юрид.н., доц.



А. Р. Салимгареева

Разработчик программы,
старший преподаватель



Л. Н. Буйлушкина

1. Цели и задачи дисциплины

Целью дисциплины «Основы информационной безопасности» является: - изучение основных направлений защиты компьютерной информации; - изучение организационных и административных методов защиты информации; - изучение программно-аппаратных средств защиты компьютерных систем; - обзор готовых решений по обеспечению информационной безопасности, разработка программных средств аудита безопасности, выявления вторжений и программных средств криптографической защиты информации. Задачами дисциплины являются: - дать знания студентам по основным угрозам безопасности компьютерных систем; - дать знания основных стандартов безопасности компьютерных систем; - дать знания моделей безопасности компьютерных систем; - дать знания основных криптографических систем; - дать знания основ администрирования сетей и защиты информации в сетях.

Краткое содержание дисциплины

Основы информационной безопасности и защита информации. История криптографии. Основные термины и определения. Классификация шифров. Шифры замены. Шифры перестановки. Шифры гаммирования. Комбинированные шифры. Шифрование с открытым ключом. Хеш-функции. Криптографические протоколы. протоколы обмена ключами. Протоколы аутентификации (идентификации). Протоколы электронной цифровой подписи. Протоколы контроля целостности. Протоколы электронных платежей. Протоколы голосования. Другие протоколы. Некоторые сведения из теорий алгоритмов и чисел. Основы криптоанализа. Стеганография. Кодирование информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-3 Способен разрабатывать компоненты системных программных продуктов на основе соответствующей технической документации	Знает: современные подходы к обеспечению информационной безопасности; основы информационной защиты, иметь понятие о компьютерных преступлениях и их классификации, методы и алгоритмы тестирования, и элементы диагностирования неисправностей, криптографические методы защиты Умеет: пользоваться современной научно-технической информацией, применять полученные знания. Имеет практический опыт: в построении систем обеспечения информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Программирование на языке C++	Технологии хранилищ данных,

	Технологии аналитической обработки информации, Введение в искусственный интеллект, Автоматизация деятельности предприятия, Производственная практика (преддипломная) (8 семестр)
--	---

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

Дисциплина	Требования
Программирование на языке С++	Знает: синтаксис языка С++ и технологии разработки прикладного ПО на языке С++, среды разработки на языке С++, алгоритмы и структуры данных в языке С++; библиотеки машинного обучения на языке С++ Умеет: разрабатывать прикладные программные решения на языке С++, разрабатывать ПО на языке С++ с использованием системных вызовов (API операционных систем), реализовывать алгоритмы сбора, анализа и обработки данных с применением библиотек С++ Имеет практический опыт: создания приложений на языке С++ с соблюдением принципов ООП и code style, применять методики использования программных средств для решения практических задач; в разработке компонентов программных комплексов, применения библиотек машинного обучения при разработке приложений искусственного интеллекта на С++

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
<i>Аудиторные занятия:</i>	48	48
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	53,75	53,75
Подготовка реферата, презентации	33,75	33,75
Подготовка к зачету	20	20
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	Основы информационной безопасности и защита информации.	6	4	2	0
2	История криптографии. Основные термины и определения. Классификация шифров	6	4	2	0
3	Шифры замены. Шифры перестановки. Шифры гаммирования. Комбинированные шифры. Шифрование с открытым ключом.	8	6	2	0
4	Хеш-функции.	6	4	2	0
5	Криптографические протоколы. протоколы обмена ключами. Протоколы аутентификации (идентификации). Протоколы электронной цифровой подписи.	10	6	4	0
6	Протоколы контроля целостности. Протоколы электронных платежей. Протоколы голосования. Другие протоколы.	6	4	2	0
7	Некоторые сведения из теорий алгоритмов и чисел. Основы криптоанализа. Стеганография. Кодирование информации.	6	4	2	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1,2	1	Основы информационной безопасности: Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации.	4
3,4	2	История криптографии: Наивная криптография, формальная криптография, математическая криптография. Основные термины и определения: Классификация шифров. Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем.	4
5,6,7	3	Шифры замены: Основы шифрования, шифры: однозначной замены, полиалфавитные, омофонические, полиалфавитные. Шифры перестановки: Основы шифрования, шифры одинарной и множественной перестановки. Шифры гаммирования: Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм. Комбинированные шифры: Основы шифрования, ADFGX, DES, ГОСТ 28147-89. Шифрование с открытым ключом: Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамала, алгоритм на основе эллиптических кривых.	6
8,9	4	Хеш-функции: Основные понятия, MD5, применение шифрования для получения хеш-образа	4
10,11,12	5	Криптографические протоколы. протоколы обмена ключами: Основные сведения о криптографических протоколах, протоколы обмена ключами. Протоколы аутентификации (идентификации): Общие сведения, парольная идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер аутентификации Kerberos, идентификация / аутентификация с помощью	6

		биометрических данных, идентификационные карты (ID-cards) и электронные ключи. Протоколы электронной цифровой подписи: Общие сведения, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ 34.10-2001, разновидности ЭЦП.	
13,14	6	Протоколы контроля целостности: Общие сведения, использование контрольных сумм, использование ЭЦП, использование MAC-кодов, проверка четности, использование ECC, комбинированные методы. Протоколы электронных платежей: Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошельки в Internet, цифровые деньги. Протоколы голосования: Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования. Другие протоколы: Протокол разделения секрета, протокол подбрасывания монеты "по телефону", тайные многосторонние вычисления.	4
15,16	7	Некоторые сведения из теорий алгоритмов и чисел: Сложность алгоритмов, простые числа, разложение числа на простые сомножители, нахождение начального списка простых чисел, тестирование числа на простоту, определение наибольшего общего делителя. Основы криптоанализа: Угрозы безопасности при использовании криптографии, общие сведения о криптоанализе, разновидности атак на криптосистемы. Стеганография: Общие сведения, классическая стеганография, компьютерная стеганография. Кодирование информации: Общие сведения, общедоступные и секретные кодовые системы, номенклатуры.	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Основы информационной безопасности: Информация и информационная безопасность, основные составляющие информационной безопасности, объекты защиты, категории и носители информации, средства защиты информации.	2
2	2	История криптографии: Наивная криптография, формальная криптография, математическая криптография. Основные термины и определения: Классификация шифров. Основные термины и определения, основные требования к криптосистемам, классификация криптографических систем.	2
3	3	Шифры замены: Основы шифрования, шифры: однозначной замены, полиалфавитные, омофонические, полиалфавитные. Шифры перестановки: Основы шифрования, шифры одинарной и множественной перестановки. Шифры гаммирования: Основы шифрования, шифрование по модулю N и 2, генерация гаммы, генераторы гамм. Комбинированные шифры: Основы шифрования, ADFGX, DES, ГОСТ 28147-89. Шифрование с открытым ключом: Основы шифрования, алгоритм RSA, алгоритм на основе задачи об укладке ранца, вероятностное шифрование, алгоритм шифрования Эль-Гамала, алгоритм на основе эллиптических кривых.	2
4	4	Хеш-функции: Основные понятия, MD5, применение шифрования для получения хеш-образа	2
5,6	5	Криптографические протоколы. протоколы обмена ключами: Основные сведения о криптографических протоколах, протоколы обмена ключами. Протоколы аутентификации (идентификации): Общие сведения, парольная идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер	4

		аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи. Протоколы электронной цифровой подписи: Общие сведения, протокол на базе алгоритма RSA, алгоритм цифровой подписи ГОСТ 34.10-94, алгоритм цифровой подписи ГОСТ 34.10-2001, разновидности ЭЦП.	
7	6	Протоколы контроля целостности: Общие сведения, использование контрольных сумм, использование ЭЦП, использование MAC-кодов, проверка четности, использование ECC, комбинированные методы. Протоколы электронных платежей: Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошельки в Internet, цифровые деньги. Протоколы голосования: Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования. Другие протоколы: Протокол разделения секрета, протокол подбрасывания монеты "по телефону", тайные многосторонние вычисления.	2
8	7	Некоторые сведения из теорий алгоритмов и чисел: Сложность алгоритмов, простые числа, разложение числа на простые сомножители, нахождение начального списка простых чисел, тестирование числа на простоту, определение наибольшего общего делителя. Основы криптоанализа: Угрозы безопасности при использовании криптографии, общие сведения о криптоанализе, разновидности атак на криптосистемы. Стеганография: Общие сведения, классическая стеганография, компьютерная стеганография. Кодирование информации: Общие сведения, общедоступные и секретные кодовые системы, номенклатуры.	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
Подготовка реферата, презентации	ЭУМД ОСН. 1 стр. 25-65; стр. 75-87; стр. 111-130; стр. 93-101; стр. 183-210; ЭУМД доп. 1 стр. 41-95; стр. 131-148	3	33,75
Подготовка к зачету	ЭУМД ОСН. 1 стр. 25-65; стр. 75-87; стр. 111-130; стр. 93-101; стр. 183-210; ЭУМД осн. 2 стр. 7-14; стр. 15-39 ЭУМД доп. 1 стр. 41-51;	3	20

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	3	Текущий контроль	Шифрование, дешифрование информации с применением комбинированных криптографических алгоритмов	1	5	Защита практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается правильность выполнения задания, качество оформления, правильность выводов и ответы на вопросы (задаются 2 вопроса). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179 с учетом редакций) Общий балл при оценке складывается из следующих показателей зачет (за каждую практическую работу): - задание выполнено правильно – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 1 балл	зачет
2	3	Текущий контроль	Режимы работы блочных шифров. Схемы кратного шифрования	1	5	Защита практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается правильность выполнения задания, качество оформления, правильность выводов и ответы на вопросы (задаются 2 вопроса). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179 с учетом редакций) Общий балл при оценке складывается из следующих показателей зачет (за каждую практическую работу): - задание выполнено правильно – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 1 балл	зачет
3	3	Текущий контроль	Дешифрование заданной фразы с применением	1	5	Защита практического задания осуществляется индивидуально. Студентом предоставляется	зачет

			известного криптографического алгоритма			оформленный отчет. Оценивается правильность выполнения задания, качество оформления, правильность выводов и ответы на вопросы (задаются 2 вопроса). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179 в ред. от 27.02.2024) Общий балл при оценке складывается из следующих показателей зачет (за каждую практическую работу): - задание выполнено правильно – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 1 балл	
4	3	Текущий контроль	Программная реализация криптографических протоколов	1	5	Защита практического задания осуществляется индивидуально. Студентом предоставляется оформленный отчет. Оценивается правильность выполнения задания, качество оформления, правильность выводов и ответы на вопросы (задаются 2 вопроса). При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179 с учетом редакций) Общий балл при оценке складывается из следующих показателей зачет (за каждую практическую работу): - задание выполнено правильно – 1 балл - выводы логичны и обоснованы – 1 балл - оформление работы соответствует требованиям – 1 балл - правильный ответ на один вопрос – 1 балл	зачет
5	3	Проме- жуточная аттестация	Зачет	-	100	На зачете происходит оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. При оценивании результатов учебной деятельности обучающегося по дисциплине используется балльно- рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом	зачет

					ректора от 24.05.2019 г. № 179 с учетом редакций) Зачтено: рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: рейтинг обучающегося за мероприятие менее 60 %	
--	--	--	--	--	--	--

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	При оценивании результатов учебной деятельности по дисциплине используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179 с учетом редакций). На аттестационном мероприятии (зачет) проводится оценивание учебной деятельности обучающихся по дисциплине на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля. Индивидуальный рейтинг обучающегося является основанием для выставления оценки по промежуточной аттестации. Рейтинг обучающегося по дисциплине определяется только по результатам текущего контроля. Студент вправе пройти контрольное мероприятие в рамках промежуточной аттестации для улучшения своего рейтинга. Зачтено: рейтинг обучающегося за мероприятие больше или равен 60 %. Не зачтено: рейтинг обучающегося за мероприятие менее 60 %	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ				
		1	2	3	4	5
ПК-3	Знает: современные подходы к обеспечению информационной безопасности; основы информационной защиты, иметь понятие о компьютерных преступлениях и их классификации, методы и алгоритмы тестирования, и элементы диагностирования неисправностей, криптографические методы защиты	+	+	+	+	+
ПК-3	Умеет: пользоваться современной научно-технической информацией, применять полученные знания.	+	+	+	+	+
ПК-3	Имеет практический опыт: в построении систем обеспечения 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. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей [Текст]/ В.Ф. Шаньгин.- М.: ИД «ФОРУМ»: ИНФРА-М, 2011.- 416 с. - ISBN 978-5 8199-0331-5
2. Малюк, А.А. Введение в защиту информации в автоматизированных системах [Текст]: учебное пособие для вузов / А.А. Малюк, С.В. Пазизин, Н.С.Погожин. – 2-е изд. – М.: Горячая линия – Телеком, 2004. – 147с.: ил.- ISBN 5-93517-062-0.
3. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах [Текст]: учебное пособие для студентов вузов / П.Б. Хорев.- М.: Академия, 2006.- 256с.- ISBN 5-7695-1839-1.

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

г) методические указания для студентов по освоению дисциплины:

1. Защита информации и криптография: методические указания по выполнению самостоятельной работы для обучающихся по направлению 09.03.04 Программная инженерия / сост. Л.Н.Буйлушкина – Нижневартонск, 2022. – 11 с.

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Защита информации и криптография: методические указания по выполнению самостоятельной работы для обучающихся по направлению 09.03.04 Программная инженерия / сост. Л.Н.Буйлушкина – Нижневартонск, 2022. – 11 с.

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	ЭБС издательства Лань	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. https://e.lanbook.com/book/156401
2	Дополнительная литература	ЭБС издательства Лань	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. https://e.lanbook.com/book/207095
3	Основная литература	Образовательная платформа Юрайт	Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — ISBN 978-5-534-16388-9. https://urait.ru/bcode/567915
4	Основная литература	Электронно-библиотечная система Znanium.com	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — ISBN 978-5-369-01761-6. https://znanium.ru/catalog/product/208264

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)
2. ФГАОУ ВО "ЮУрГУ (НИУ)"-Портал "Электронный ЮУрГУ" (<https://edu.susu.ru>)(бессрочно)
3. -Borland Developer Studio(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "Консультант Плюс Югра"-Консультант Плюс (Нижневартовск)(31.12.2026)

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		Предустановленное программное обеспечение: ОС Windows 7 Professional; Денвер; MS SQL Server 2008R2; Oracle VM VirtualBox; Microsoft Office 2010; Информационно-правовая база «Консультант – Плюс»; DOSBox
Зачет		Предустановленное программное обеспечение: ОС Windows 7 Professional; Денвер; MS SQL Server 2008R2; Oracle VM VirtualBox; Microsoft Office 2010; Информационно-правовая база «Консультант – Плюс»; DOSBox
Лекции		Занятия студентов проходят в лекционных и компьютерных аудиториях филиала. Основная и дополнительная литература, словари находятся в фондах библиотеки филиала, где также организован доступ к материалам электронных библиотечных систем