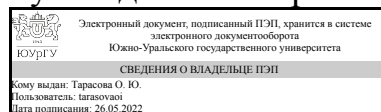


ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Руководитель направления



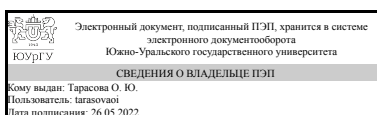
О. Ю. Тарасова

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.17 Криптографические методы защиты информации
для направления 09.03.04 Программная инженерия
уровень Бакалавриат
форма обучения очная
кафедра-разработчик Математика и вычислительная техника

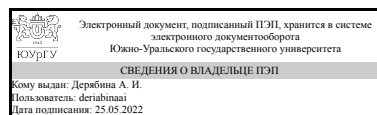
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.04 Программная инженерия, утверждённым приказом Минобрнауки от 19.09.2017 № 920

Зав.кафедрой разработчика,
к.физ.-мат.н., доц.



О. Ю. Тарасова

Разработчик программы,
к.техн.н., доцент



А. И. Дерябина

1. Цели и задачи дисциплины

Целью дисциплины является: получить систематизированное представление об основах обеспечения информационной безопасности (ИБ); обеспечить базовый уровень подготовки, необходимый для анализа угроз и эффективности систем защиты информационных систем (ИС), оценки уровня защищенности ИС, планирования организационных мероприятий и установки программно-аппаратных средств защиты ИС, а также для самостоятельного изучения методов и средств обеспечения информационной безопасности (ИБ) при создании и эксплуатации информационных систем различного назначения. Изучение дисциплины способствует формированию информационной культуры; предполагает изучение теоретических основ, принципов реализации и использования современных методов и средств обеспечения информационной безопасности. Задачи дисциплины - изучение нормативных документов по защите информации в информационных системах; - изучение видов угроз информационным технологиям; - изучение методов и способов; - защиты информации в информационно-телекоммуникационных системах; - защиты информации от несанкционированного доступа; - криптографической защиты информации; - защиты информации при межсетевом взаимодействии, особенности защиты персональных данных в информационных системах; - изучить назначение, цели и порядок проведения аудита информационной безопасности; - назначения и порядок использования средств электронно-цифровой подписи при ведении электронного документооборота. В результате освоения дисциплины студент должен Знать: - основные понятия и направления в защите компьютерной информации; - принципы защиты информации; - принципы классификации и примеры угроз безопасности компьютерным системам; - современные подходы к защите продуктов и систем информационных технологий, реализованные в действующих отечественных и международных стандартах ИТ-безопасности; - основные инструменты обеспечения многоуровневой безопасности в информационных системах; - современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования; - состав и организацию систем информационной безопасности; - методы криптографических преобразований; - основные стандарты и протоколы шифрования и электронной подписи. Уметь: - проводить анализ потенциально возможных угроз информации и информационным технологиям информационных систем; - выбирать эффективные способы и средства защиты информации; - использовать нормативные документы в области защиты информации и информационной безопасности; - проводить анализ результатов аудита информационной безопасности; - организовывать работу по защите персональных данных в организации; - конфигурировать встроенные средства безопасности в операционной системе; - устанавливать и использовать средства для шифрования информации и организации обмена данными с использованием электронной цифровой подписи, межсетевые экраны; - устанавливать и настраивать программное обеспечение для защиты от вредоносного программного обеспечения; - настроить инструменты резервного копирования и восстановления информации; - выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты. Владеть: - методами аудита безопасности информационных систем; - методами системного анализа

информационных систем; - навыками работы с техническими и программными средствами защиты информации.

Краткое содержание дисциплины

Дисциплина "Криптографические методы защиты информации" принадлежит к циклу дисциплин общепрофессиональной подготовки и включает следующие основные разделы: Классификация средств защиты информации и программного обеспечения. Криптографические модели и методы защиты информации. Защита информации в современных ОС. Защита информации в сети. Правовые основы защиты информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-4 Способен использовать методы и инструментальные средства исследования объектов профессиональной деятельности	Знает: принципы и методы криптографической защиты информации Умеет: применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защиты информации Имеет практический опыт: организации и обеспечения режима секретности; технической защиты информации; формирования требований по защите информации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.Ф.01 Математическая логика и теория алгоритмов, 1.Ф.15 Цифровая обработка изображений, 1.Ф.10 Теория, методы и средства параллельной обработки информации, 1.Ф.04 Вычислительные методы, 1.Ф.05 Дискретная математика, 1.Ф.03 Структуры и алгоритмы обработки данных, ФД.01 Академия интернета вещей, ФД.02 Программирование параллельных программных приложений	Не предусмотрены

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

Дисциплина	Требования
1.Ф.05 Дискретная математика	Знает: основные понятия и методы дискретной математики: множества, функции и отношения;

	основы теории графов; элементы комбинаторики; основы переключательных функций. Умеет: анализировать и представлять функции и отношения в дискретных моделях; анализировать и определять тип конечных графов; анализировать и выявлять тип комбинаторных конфигураций; минимизировать переключательные функции Имеет практический опыт: использования методов и средств дискретной математики в профессиональной деятельности
1.Ф.03 Структуры и алгоритмы обработки данных	Знает: основные типы структур данных, используемые в мировой практике программирования; способы отображения структур данных на структуры хранения; основные операции и алгоритмы над структурами Умеет: применять изученные типы данных и алгоритмы работы с ними при решении конкретных задач; оценивать затраты времени и ресурсов при использовании тех или иных структур и алгоритмов в существующих и вновь разрабатываемых программных средствах Имеет практический опыт: программирования операций над основными базовыми структурами данных при программировании конкретных задач
1.Ф.15 Цифровая обработка изображений	Знает: Алгоритмы обработки цифровых изображений, стандартные библиотеки сред разработки Умеет: Применять базовые алгоритмы цифровой обработки изображений Имеет практический опыт: обработки цифровых изображений с использованием информационных технологий
1.Ф.01 Математическая логика и теория алгоритмов	Знает: теоретические основы математической логики и теории алгоритмов Умеет: использовать логические методы исследования для построения и реализации плана решения задачи профессиональной деятельности Имеет практический опыт: применения математической логики и теории алгоритмов в профессиональной деятельности
1.Ф.10 Теория, методы и средства параллельной обработки информации	Знает: технологии параллельного и распределенного программирования; проблемы балансировки загрузки вычислительных узлов при распределенном программировании. , теорию, методы и средства параллельной обработки информации Умеет: разрабатывать параллельные алгоритмы для разного класса задач , разрабатывать параллельные алгоритмы для разного класса задач Имеет практический опыт: разработки параллельных программ OpenMP, параллельной обработки информации
1.Ф.04 Вычислительные методы	Знает: методы вычислительной математики, математические методы для решения задач автоматизированного проектирования и при

	разработке математического обеспечения средств вычислительной техники Умеет: решать задачи вычислительной математики с применением пакетов для научных и инженерных расчетов , решать задачи вычислительной математики с применением пакетов для научных и инженерных расчетов Имеет практический опыт: применения вычислительных методов при решении прикладных задач , использования инструментальных средств систем компьютерной математики; применения вычислительных методов при решении прикладных задач
ФД.02 Программирование параллельных программных приложений	Знает: технологии параллельного программирования; технологии MPI и OpenMP, основные подходы к разработке параллельных программ; основные технологии и модели параллельного программирования; методы создания параллельных программ для типичных задач многопоточного программирования Умеет: разрабатывать параллельные алгоритмы для разного класса задач; использовать библиотеки для реализации технологий MPI и OpenMP, применять общие схемы разработки параллельных программ для реализаций собственных алгоритмов; проводить распараллеливание вычислительных алгоритмов; оценивать эффективность параллельных вычислений Имеет практический опыт: в области параллельного программирования, создания параллельных программ
ФД.01 Академия интернета вещей	Знает: терминологию, принятую в изучаемой дисциплине; ее основные понятия и определения; применяемые на практике алгоритмы и методы., терминологию, принятую в изучаемой дисциплине, ее основные понятия и определения, применяемые на практике алгоритмы и математические методы; терминологию, принятую в изучаемой дисциплине, ее основные понятия и определения, применяемые на практике алгоритмы и математические методы; Умеет: разбираться в существующих IoT-технологиях и применять их к конкретным сценариям , Организовать сбор и обработку данных, необходимых для функционирования системы на базе IoT-устройств при решении профессиональных задач., организовать сбор и обработку данных, необходимых для функционирования системы на базе IoT-устройств при решении профессиональных задач. Имеет практический опыт: базовыми навыками программирования конечных устройств , проектирования и реализация элементов систем на базе IoT-устройств, проектирования и реализация элементов систем

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч., 66,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	108	108
<i>Аудиторные занятия:</i>	60	60
Лекции (Л)	24	24
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36
Лабораторные работы (ЛР)	0	0
<i>Самостоятельная работа (СРС)</i>	41,75	41,75
Изучение тем, вынесенных на самостоятельную проработку	17,75	17.75
Подготовка к зачету	8	8
Подготовка к выполнению, оформление индивидуальных заданий практических работ	16	16
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	Источники, риски и формы атак на компьютерные системы	4	4	0	0
2	Модели безопасности информационных систем	4	4	0	0
3	Стандарты безопасности. Правовые основы защиты информации	4	4	0	0
4	Криптографические модели и методы защиты информации	26	6	20	0
5	Защита информации в современных ОС	12	2	10	0
6	Защита информации в сети	10	4	6	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Понятие информационной безопасности. Функции и задачи защиты информации. Методы и системы защиты информации. Основные виды угроз безопасности. Классификация атак на вычислительные системы. Сетевые атаки. Компьютерные вирусы и антивирусные программы.	2

2	1	Понятие угрозы. Классификация угроз. Аспекты ИБ: доступность, целостность, конфиденциальность. Угрозы доступности. Угрозы целостности. Угрозы конфиденциальности.	2
3,4	2	Виды политик безопасности. Дискреционные модели. Виды политик безопасности. Дискреционные модели. Мандатные модели. Модель ролевого доступа	4
5,6	3	Назначение и задачи в сфере обеспечения ИБ на уровне государства. Правовые документы РФ по ИБ. Материалы Гостехкомиссии РФ. Единые критерии безопасности информационных технологий	4
7	4	Классическая криптография. Симметричные криптосистемы. Блочные и поточные шифры на примере алгоритмов RC4, DES, Triple DES, AES. Шифрование на основе паролей. Понятие ключа. Аппаратные устройства хранения ключей. Безопасное распределение ключей. Инфраструктура управления открытыми ключами	2
8	4	Ассиметричные алгоритмы шифрования. Одностронние функции в ассиметричных криптосистемах. Алгоритм RSA, алгоритм эллиптических кривых Диффи-Хеллмана.	2
9	4	Сжатие данных как способ кодирования информации. Кодирование Хаффмена. Адаптивное сжатие по Хаффмену. Арифметическое кодирование. Алгоритм сжатия Lempel-Ziv-Welch.	2
10	5	Защита информации в ОС Windows. Защита информации в ОС Linux. Система Kerberos	2
11	6	Проблемы безопасности протоколов TCP/IP. Сетевые атаки. Система обнаружения атак. Средства анализа защищенности сетевого ПО.	2
12	6	Защита информации на транспортном уровне семиуровневой модели ISO/OSI. Протокол SSL/TLS. Защита информации на прикладном уровне семиуровневой модели ISO/OSI. Протокол SMIME и система PGP. Межсетевые экраны. Система отслеживания вторжений. Аудит и мониторинг безопасности	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1,2,3	4	Шифрование, дешифрование информации с применением комбинированных криптографических алгоритмов	6
4,5	4	Криптографические алгоритмы, применяемые в аппаратных устройствах шифрования	4
6,7,8	4	Дешифрование заданной фразы с применением известного криптографического алгоритма	4
9,10	4	Блочные алгоритмы шифрования информации на основе сетей Фейстеля	4
11,12	4	Ассиметричные алгоритмы шифрования на основе односторонней функции	2
13	5	Управление правами в ОС Windows XP	4
14	5	Анализ сетевой активности с помощью Командной строки	6
15,16	6	Архитектура корпоративных почтовых систем и протоколов	6

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
Изучение тем, вынесенных на самостоятельную проработку	Осн лит: №2 (с.155-180, с. 211-227, с. 232-240), №3 (с. 76-86, с. 148-178), Доп.лит.: №1 (Главы 4,5,6,7,10,12,13)	8	17,75
Подготовка к зачету	Осн лит: №2 (с.155-180, с. 211-227, с. 232-240), №3 (с. 76-86, с. 148-178), Доп.лит.: №1 (Главы 4,5,6,7,10,12,13)	8	8
Подготовка к выполнению, оформление индивидуальных заданий практических работ	Осн лит: №2 (с.155-180, с. 211-227, с. 232-240), №3 (с. 76-86, с. 148-178), Доп.лит.: №1 (Главы 4,5,6,7,10,12,13)	8	16

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	8	Текущий контроль	Криптографические модели и методы защиты информации	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	зачет
2	8	Текущий контроль	Защита информации в современных ОС	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	зачет
3	8	Текущий контроль	Защита информации в сети	1	15	13-15 баллов - практические навыки работы с освоенным материалом полностью сформированы 11-13 баллов - практические навыки работы с освоенным материалом сформированы недостаточно 9-11 баллов - необходимые практические навыки работы с освоенным материалом в	зачет

						основном сформированы	
4	8	Промежуточная аттестация	зачет	-	0	При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Зачет выставляется по накоплению баллов за мероприятия текущего контроля Зачтено: рейтинг обучающегося за мероприятия текущего контроля больше или равно 60 %. Не зачтено: рейтинг обучающегося за мероприятия текущего контроля менее 60 %	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	В течение семестра студенты выполняют 3 практические работы, которые участвуют в формировании итоговой оценки за семестр. Для расчета итоговых оценок все оценки за лабораторные работы представляются в виде доли от максимального балла конкретного задания, выраженной в процентах. Итоговая оценка за семестр определяется как среднее арифметическое оценок за задания семестра. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179), согласно с пп. 2.5, 2.6 Положения	В соответствии с пп. 2.5, 2.6 Положения

6.3. Паспорт фонда оценочных средств

Компетенции	Результаты обучения	№ КМ			
		1	2	3	4
ПК-4	Знает: принципы и методы криптографической защиты информации				+
ПК-4	Умеет: применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защиты информации				+
ПК-4	Имеет практический опыт: организации и обеспечения режима секретности; технической защиты информации; формирования требований по защите информации				+

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. Вестник Южно-Уральского государственного университета.
Серия: Математика. Механика. Физика [Электронный ресурс] / Юж.-Урал. гос. ун-т. – Электрон. дан. – Челябинск : Изд-во ЮУрГУ. – 2003 – Режим доступа: https://e.lanbook.com/journal/2547#journal_name. – Загл. с экрана.

2. Вестник Южно-Уральского государственного университета.
Серия: Математическое моделирование и программирование [Электронный ресурс] / Юж. - Урал.гос.ун-т. -Электрон.дан. - Челябинск: Изд-во ЮУрГУ. - 2008-2016 - Режим доступа: https://e.lanbook.com/journal/2548#journal_name - Загл. с экрана

г) методические указания для студентов по освоению дисциплины:

1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие/ П.Н.Девянин. - М: "Горячая линия-Телеком", 2012. - 320с.

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие/ П.Н.Девянин. - М: "Горячая линия-Телеком", 2012. - 320с.

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Дополнительная литература	Электронно-библиотечная система издательства Лань	Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/176563
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 (дата обращения: 31.01.2022).
3	Основная литература	Электронно-библиотечная система издательства Лань	Каширская, Е. Н. Криптографический анализ и методы защиты информации : учебное пособие / Е. Н. Каширская. — Москва : РТУ МИРЭА, 2020. — 91 с. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/163861

Перечень используемого программного обеспечения:

1. Microsoft-Office(бессрочно)

2. -Visual Studio 2017 Community(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
Самостоятельная работа студента	202 (3)	ПК в составе (12 шт): Корпус MidiTower Inwin C583 350W Grey Процессор Intel Core 2 Duo E4600, 2,4GHz, 2Mb, 800MHz Socket-775 BOX. Мат.плата ASUS P5KPL-VM, Socket 775.Память 1024Mb PC2-5300(667Mhz) SEC-1. Жесткий диск 160,0 Gb HDD Seagate (ST3160815AS) Barracuda7200.10 8Mb SATA-300 Привод DVD±RW Samsung SH-S202J. Клавиатура Genius (KB-06XE), PS/2, White. Мышь Genius NetScroll 110 white optical (800dpi) PS/2. Монитор 17" Samsung 720N VKS TFT; Системный блок (1 шт): "Стандарт" * (без фильтра для ethernet, без считывателя); Монитор (1 шт): MONITOR Acer V193WV Cb; Проектор (1 шт) Acer X1263; Проекционный экран (1 шт).
Практические занятия и семинары	203 (3)	ПК в составе (12 шт): Корпус MidiTower Inwin C583 350W Grey Процессор Intel Core 2 Duo E4600, 2,4GHz, 2Mb, 800MHz Socket-775 BOX. Мат.плата ASUS P5KPL-VM, Socket 775.Память 1024Mb PC2-5300(667Mhz) SEC-1. Жесткий диск 160,0 Gb HDD Seagate (ST3160815AS) Barracuda7200.10 8Mb SATA-300 Привод DVD±RW Samsung SH-S202J. Клавиатура Genius (KB-06XE), PS/2, White. Мышь Genius NetScroll 110 white optical (800dpi) PS/2. Монитор 17" Samsung 720N VKS TFT; Системный блок (1 шт): "Стандарт" * (без фильтра для ethernet, без считывателя); Монитор (1 шт): MONITOR Acer V193WV Cb; Проектор (1 шт) Acer X1263; Проекционный экран (1 шт).
Лекции	203 (3)	ПК в составе (12 шт): Корпус MidiTower Inwin C583 350W Grey Процессор Intel Core 2 Duo E4600, 2,4GHz, 2Mb, 800MHz Socket-775 BOX. Мат.плата ASUS P5KPL-VM, Socket 775.Память 1024Mb PC2-5300(667Mhz) SEC-1. Жесткий диск 160,0 Gb HDD Seagate (ST3160815AS) Barracuda7200.10 8Mb SATA-300 Привод DVD±RW Samsung SH-S202J. Клавиатура Genius (KB-06XE), PS/2, White. Мышь Genius NetScroll 110 white optical (800dpi) PS/2. Монитор 17" Samsung 720N VKS TFT; Системный блок (1 шт): "Стандарт" * (без фильтра для ethernet, без считывателя); Монитор (1 шт): MONITOR Acer V193WV Cb; Проектор (1 шт) Acer X1263; Проекционный экран (1 шт).