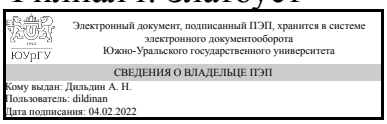
ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор филиала
Филиал г. Златоуст



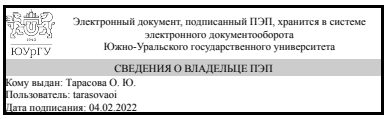
А. Н. Дильдин

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.12 Программирование защищенных информационных систем
для направления 09.03.04 Программная инженерия
уровень Бакалавриат
форма обучения очная
кафедра-разработчик Математика и вычислительная техника

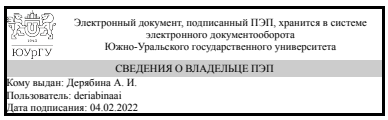
Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 09.03.04 Программная инженерия, утверждённым приказом Минобрнауки от 19.09.2017 № 920

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



О. Ю. Тарасова

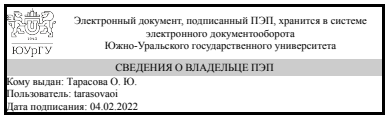
Разработчик программы,
к.техн.н., доцент



А. И. Дерябина

СОГЛАСОВАНО

Руководитель направления
к.физ.-мат.н., доц.



О. Ю. Тарасова

Златоуст

1. Цели и задачи дисциплины

Формирование у обучаемых знаний в области теоретических основ информационной безопасности (ИБ) и защиты информации (ЗИ), умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в системах защиты информации (СЗИ) в вычислительных системах и сетях (ВСС). Цель изучения дисциплины достигается путем решения следующих задач: изучение теоретических положений ИБ, ее средств и методов, особенностей их использования в ВСС, перспектив развития в информационных технологий (ИТ), предметной и смежных с ней областях; повышения уровня профессиональной культуры и исполнительской дисциплины бакалавров, понимание необходимости использования СЗИ в ВВС, в профессиональной деятельности по специальности; освоения основные средств и методов обеспечения ИБ, методик их результативного использования; изучения технических и программно-аппаратных средств ЗИ, их основных характеристик; приобретения умений и навыков работы с СЗИ

Краткое содержание дисциплины

Дисциплина посвящена изучению существующих технологий и программно-аппаратных средств защиты компьютерных сетей. В содержание дисциплины входят четыре основные направления: Комплексный подход к обеспечению информационной безопасности. Методы и средства обеспечения безопасности информации. Компьютерные вирусы и средства антивирусной защиты. Стандарты защищенности информации в компьютерных системах. В ходе изучения дисциплины студенты получают знания о современных технологиях защиты информации. Также студенты учатся разбираться с многообразием законодательных актов Российской Федерации и международных стандартах в области защиты информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-1 ПК-1 демонстрировать понимание концепций и атрибутов качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов , инструментов и технологий обеспечения качества	Знает: методы обнаружения вторжений в информационные системы (ИС); методы безопасного использования коммуникационных сетей общего доступа при построении защищенных ИС; основные принципы применения аппаратных и программных средств обеспечения информационной безопасности Умеет: применять современные программные и аппаратные средства защиты информации; классифицировать и оценивать угрозы информационной безопасности для ИС Имеет практический опыт: работы с ведущими программными и аппаратными комплексными средствами защиты информации

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
1.О.15.02 Программирование на языках высокого уровня	1.Ф.17 Криптографические методы защиты информации

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

Дисциплина	Требования
1.О.15.02 Программирование на языках высокого уровня	Знает: основы высокоуровневого языка программирования, методы отладки программ, основные понятия концепции качества программного обеспечения, характеристики качества и их атрибуты Умеет: проводить структурную декомпозицию задач, применять конструкции языка высокого уровня для решения задач по заданному или разработанному алгоритму, разрабатывать структурные программы, удовлетворяющие требованиям качества (функциональным и нефункциональным) Имеет практический опыт: программирования на языке высокого уровня, а так же навыки отладки и тестирования программ, применения языковых конструкций в разработке, отладке и тестировании программ

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч., 74,5 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		6
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	69,5	69,5
с применением дистанционных образовательных технологий	0	
Подготовка к практическим занятиям	20	20
Изучение тем, вынесенных на самостоятельную проработку	25,5	25.5
Подготовка к экзамену	24	24
Консультации и промежуточная аттестация	10,5	10,5

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	Комплексный подход к обеспечению информационной безопасности	18	6	12	0
2	Методы и средства обеспечения безопасности информации	18	10	8	0
3	Компьютерные вирусы и средства антивирусной защиты	14	8	6	0
4	Стандарты защищенности информации в компьютерных системах	14	8	6	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Введение в проблему информационной безопасности, ее актуальности. Основные объекты информационных систем, подлежащие защите. Цели и задачи обеспечения информационной безопасности для различных объектов	2
2	1	Основные понятия информационной безопасности. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность. Комплексный подход к защите информации. Уровни формирования режима информационной безопасности: законодательный, административный, процедурный и программно-технический. Требования к комплексным системам защиты информации.	2
3	1	Компьютерная система как объект защиты информации. Понятие угрозы информационной безопасности в компьютерных системах. Классификация и общий анализ угроз информационной безопасности в компьютерных системах. Случайные угрозы информационной безопасности. Преднамеренные угрозы информационной безопасности. Административный, процедурный и программно-технический уровни информационной безопасности. Административный, процедурный и программно-технический уровни информационной безопасности	2
4,5	2	Основные виды технических каналов утечки информации. Техника промышленного шпионажа. Противодействие наблюдению. Противодействие прослушиванию. Методы и средства защиты от побочных электромагнитных излучений и наводок. Способы несанкционированного доступа к информации в компьютерных системах. Характеристика средств защиты информации в компьютерных системах от несанкционированного доступа. Идентификация и аутентификация пользователей: основные понятия, парольная аутентификация, виды паролей, биометрическая аутентификация. Управление доступом: основные понятия, виды разграничения доступа, особенности дискреционного, мандатного и ролевого управления доступом.	4
6,7,8	2	Защита программных средств от несанкционированного копирования и исследования. Протоколирование и аудит: основные понятия, активный аудит. Методы аутентификации, использующие пароли. Построение системы разграничения доступа в базе данных на основе ролевой модели. Развитие криптографических систем. Основные понятия криптологии. Классификация криптографических средств. Симметричные криптосистемы: DES и ее	6

		модификации, ГОСТ 28147 – 89, принципы их построения. Ассиметричные криптосистемы: однонаправленные функции, RSA, принципы построения. Методы шифрования: замены, перестановки, аналитические, аддитивные, комбинированные. Функция хэширования. Электронная подпись и ее применение для контроля целостности программ и данных. Компьютерная стеганография и ее применение.	
9,10	3	Основные каналы распространения вирусов. Вредоносные программы и их классификация. Программные закладки и методы защиты от них. Антивирусные программные комплексы.	4
11,12	3	Общие сведения о компьютерных вирусах. Классификация компьютерных вирусов. Жизненный цикл вирусов. Методы и средства защиты от компьютерных вирусов. Методы обнаружения и удаления вирусов. Профилактика заражения вирусами компьютерных систем.	4
13,14	4	Характеристика систем стандартизации в области защиты информации. Европейские критерии безопасности информационных технологий. Документы Гостехкомиссии России по защите информации.	4
15,16	4	Оценочные стандарты и технические спецификации: «Оранжевая книга». Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1,2,3	1	Практическая работа № 1 «Хеш-функция (MD5)»	6
4,5,6	1	Практическая работа № 2 «Идентификация и аутентификация (RSA, схемы Шнорра и Фейге-Фиата-Шамира)»	6
7,8	2	Практическая работа № 3 «Контроль целостности (биты четности, контрольные цифры, CRC и ECC)»	4
9,10	2	Практическая работа № 4 «Электронная цифровая подпись (RSA, ГОСТы 34.10-94 и 34.10-2001)»	4
11,12,13	3	Практическая работа № 5 «Контроль целостности (MAC-код DES-CBC)»	6
14,15,16	4	Практическая работа № 6 «Тайные многосторонние вычисления и разделение секрета	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
Подготовка к практическим занятиям	ЭУМД Осн лит: №1 (с.155-180), ЭУМД№ 2 (с.280-298) Метод.указан.: №1, 2, 3	6	20
Изучение тем, вынесенных на самостоятельную проработку	ЭУМД Осн лит: №1 (с.155-180, с. 211-227, с. 232-240), №2 (с. 76-86, с. 148-178), №3 (Главы 5-9, 11,12,15,16,18). ЭУМД Доп.лит.: №2 (Главы 4,5,6,7,10,12,13) №3	6	25,5

	(Главы 6,7,8,9).		
Подготовка к экзамену	ЭУМД Осн лит: №1 (с.155-180), ЭУМД №2 (с.280-298), ЭУМД №3 (Главы 9,11,15). Доп.лит.: ЭУМД №1 (Урок 5,6,7,8), Метод.указан.: №1,	6	24

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	6	Текущий контроль	Практическая работа № 1 «Хеш-функция (MD5)»	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	экзамен
2	6	Текущий контроль	Практическая работа № 2 «Идентификация и аутентификация (RSA, схемы Шнорра и Фейге-Фиата-Шамира)»	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	экзамен
3	6	Текущий контроль	Практическая работа № 3 «Контроль целостности (биты четности, контрольные цифры, CRC и ECC)»	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	экзамен
4	6	Текущий контроль	Практическая работа № 4 «Электронная цифровая подпись (RSA, ГОСТы 34.10-94 и 34.10-	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	экзамен

			2001)»			баллов - необходимые практические навыки работы с освоенным материалом в основном сформированы	
5	6	Текущий контроль	Практическая работа № 5 «Контроль целостности (MAC-код DES-CBC)»	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	экзамен
6	6	Текущий контроль	Практическая работа № 6 «Тайные многосторонние вычисления и разделение секрета	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	экзамен
7	6	Проме-жуточная аттестация	Экзамен	-	130	Оценка за экзамен складывается из теоретической части (в виде ответа на 20 заданий в тестовой форме, за каждый правильный ответ 2 балла) и практической части (оценка за практические работы выполненные в течении семестра). Общая оценка за экзамен: Отлично: Более 120-130. баллов, Хорошо: от 110-120; Удовлетворительно: от 90-110; Неудовлетворительно: менее 90 баллов.	экзамен

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
экзамен	Экзамен включает в себя теоретическую и практическую части. Теоретическая часть выполняется в виде ответа на 20 заданий в тестовой форме. Практическое часть состоит из выполненных в течении семестра практических работ. Для расчета итоговой оценки баллы за ответы на тестовые вопросы и практические работы представляются в виде доли от максимального балла конкретного задания и ответа на вопрос, выраженной в процентах. Итоговая оценка за семестр определяется как среднее арифметическое оценок за задания. Зачтено: Итоговая оценка в диапазоне 70 - 100% . Не зачтено: Итоговая оценка в диапазоне 0 -69% .	В соответствии с пп. 2.5, 2.6 Положения

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ						
		1	2	3	4	5	6	7
ПК-1	Знает: методы обнаружения вторжений в информационные системы (ИС); методы безопасного использования коммуникационных сетей общего доступа при построении защищенных ИС; основные принципы применения аппаратных и программных средств обеспечения информационной безопасности	+	+	+	+	+	+	
ПК-1	Умеет: применять современные программные и аппаратные средства защиты информации; классифицировать и оценивать угрозы информационной безопасности для ИС		+		+			+
ПК-1	Имеет практический опыт: работы с ведущими программными и аппаратными комплексными средствами защиты информации			+		+		+

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:

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	Библиографическое описание

		форме	
1	Основная литература	Электронно-библиотечная система издательства Лань	Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/163844
2	Основная литература	Электронно-библиотечная система издательства Лань	Защита компьютерной информации : учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 146 с. — ISBN 978-5-907054-82-0. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/157086
3	Основная литература	Электронно-библиотечная система издательства Лань	Федин, Ф. О. Информационная безопасность баз данных : учебное пособие / Ф. О. Федин, О. В. Трубиенко, С. В. Чискидов. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 133 с. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/167605
4	Дополнительная литература	Электронно-библиотечная система издательства Лань	Методологические основы построения защищенных автоматизированных систем : учебное пособие / А. В. Душкин, О. В. Ланкин, С. В. Потехецкий, А. П. Данилкин. — Воронеж : ВГУИТ, 2013. — 263 с. — ISBN 978-5-89448-981-0. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/72890

Перечень используемого программного обеспечения:

1. Microsoft-Microsoft Imagine Premium (Windows Client, Windows Server, Visual Studio Professional, Visual Studio Premium, Windows Embedded, Visio, Project, OneNote, SQL Server, BizTalk Server, SharePoint Server)(04.08.2019)

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	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).
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).