

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
 ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
 ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
 «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
 (ФГБОУ ВО «ВГТУ», ВГТУ)

«УТВЕРЖДАЮ»
 Председатель Ученого совета факультета
 информационных технологий
 и компьютерной безопасности
 Пасмурнов С.М.
 (подпись) (ФИО)
 «30» августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информации в распределенных вычислительных системах
 (наименование дисциплины (модуля) по УП)

Закреплена за кафедрой автоматизированных и вычислительных систем

Направление подготовки: 09.04.01 Информатика и вычислительная техника
 (код, наименование)

Направленность: Распределенные автоматизированные системы
 (название магистерской программы по УП)

Часов по УП: 108; Часов по РПД: 108;

Часов по УП (без учета часов на экзамены): 108; Часов по РПД: 108;

Часов на интерактивные формы (ИФ) обучения по УП: 7 (2 – лекции, 5 – ЛР)

Часов на интерактивные формы (ИФ) обучения по РПД: 8 (2 – лекции, 5 – ЛР)

Часов на самостоятельную работу по УП: 80 (74 %);

Часов на самостоятельную работу по РПД: 80 (74 %)

Общая трудоемкость в ЗЕТ: 3;

Виды контроля в семестрах (на курсах): Экзамены - 0; Зачет - 2; Курсовые проекты - 0; Кур-
 совые работы - 0.

Форма обучения: очная; Срок обучения: нормативный.

Распределение часов дисциплины по семестрам

Вид занятий	№ семестров, число учебных недель в семестрах																	
	1 / 18		2 / 18		3 / 18		4 / 18		5 / 18		6 / 18		7 / 18		8 / 12		Итого	
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции			8	8													8	8
Лаб. раб.			20	20													20	20
Практ. занят																		
Ауд. зан.			28	28													28	28
Сам. раб			80	80													80	80
Итого			108	108													108	108

Сведения о ФГОС, в соответствии с которым разработана рабочая программа дисциплины (модуля) – 09.04.01 «Информатика и вычислительная техника», утвержден приказом Министерства образования и науки Российской Федерации от 30 октября 2014 г., № 1420.

Программу составил:  к.т.н., Сафронов В.В.
(подпись, ученая степень, ФИО)

Рецензент (ы):  к.т.н. Белозоров С.А.
(подпись, ученая степень, ФИО)

Рабочая программа дисциплины составлена на основании учебных планов подготовки магистров по направлению 09.04.01 «Информатика и вычислительная техника», направленностей «Распределенные автоматизированные системы», Методы анализа и синтеза проектных решений, Жизненный цикл изделий в едином информационном пространстве цифрового производства.

Рабочая программа обсуждена на заседании кафедры автоматизированных и вычислительных систем, протокол № 12 от « 3 » июня 2016 г.

Зав. кафедрой АВС  С.Л. Подвальный

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Цель изучения дисциплины состоит в изучении и практическом освоении методов, средств и механизмов защиты информации в распределенных автоматизированных системах.
1.2	Задачи дисциплины:
1.2.1	- ознакомление с основными методами защиты данных в распределенных автоматизированных системах;
1.2.2	- изучение основных алгоритмов, лежащих в основе систем защиты информации в распределенных вычислительных системах;
1.2.3	- приобретение навыков организации многоуровневой защиты корпоративных сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Цикл (раздел) ООП: Б1.В.ОД	Код дисциплины в УП: Б1.В.ОД.5
2.1 Требования к предварительной подготовке обучающегося	
Для успешного освоения дисциплины студент должен иметь базовую подготовку по следующим дисциплинам: сети ЭВМ и телекоммуникации, программирование.	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее	
Б1.В.ДВ.4.1	Сетевые протоколы и телекоммуникационные средства
Б1.В.ДВ.4.2	Разработка сетевых служб и протоколов
Б3	Итоговая государственная аттестация

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Код компетенции	Наименование компетенции
ПК-5	владением существующими методами и алгоритмами решения задач цифровой обработки сигналов
Владеет: методами и алгоритмами организации многоуровневой защиты информации в распределенных вычислительных системах.	
ПК-7	применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий
Знает: методы защиты информации, в том числе в распределенных вычислительных системах.	
Умеет: использовать типовые программные продукты, ориентированные на решение задач защиты информации в распределенных вычислительных системах	

В результате освоения дисциплины обучающийся должен

3.1	знать:
3.1.1	методы защиты информации, в том числе в распределенных вычислительных системах (ПК-7).
3.2	уметь:
3.2.1	использовать типовые программные продукты, ориентированные на решение задач

	защиты информации в распределенных вычислительных системах (ПК-7).
3.3	владеть:
3.3.1	методами и алгоритмами организации многоуровневой защиты информации в распределенных вычислительных системах (ПК-5).

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№	Наименование раздела дисциплины	Се- местр	Неделя семестра	Вид учебной нагрузки и их трудоемкость в часах				
				Лекции	Практические занятия	Лабораторные работы	СРС	Всего часов
1	Введение в защиту информации	2	23-26	2		8	20	30
2	Принципы построения систем защиты информации	2	27-30	2		-	20	22
3	Основы криптографии	2	31-36	2		4	20	26
4	Реализация методов защиты информации в современных распределенных системах	2	37-40	2		8	20	30
Итого				8		20	80	108

4.1 Лекции

Неделя семест- ра	Тема и содержание лекции	Объем часов	В том числе, в интерак- тивной форме (ИФ)
Второй семестр		8	2
Введение в защиту информации		2	0,5
23	Угрозы безопасности информационных систем Классификация угроз безопасности. Уязвимости информационной системы. Угрозы непосредственного доступа в операционную среду информационной системы. Угрозы безопасности межсетевое и прикладного уровня. Стандарты в области защиты информации. <i>Самостоятельное изучение. Тема 1. Стандарты в области защиты информации.</i>	2	0,5
Принципы построения систем защиты информации		2	0,5
27	Организационные, физические, программно-аппаратные средства защиты. Многоуровневая защита распределенных вычислительных систем. <i>Самостоятельное изучение. Тема 2. Идеология применения современных программно-аппаратных и физических средств защиты распределенных вычислительных систем.</i>	2	0,5
Основы криптографии		2	0,5
31	Основы криптографии	1	0,25

	Общие сведения. Подстановки. Метод перестановки. Одноразовые блокноты. Основные принципы криптографии. Алгоритмы с симметричным криптографическим ключом. Понятие об алгоритмах с симметричным криптографическим ключом. Изучение реализации на примере шифра DES. Улучшенный стандарт шифрования AES. <i>Самостоятельное изучение. Тема 3.</i> Изучение реализаций алгоритмов шифрования с открытым ключом. Изучение примеров атак на информационные системы.		
35	Работа с сертификатами. Сертификаты. Пример сертификата X.509. Инфраструктуры систем с открытыми ключами. Каталоги. Аннулирование сертификатов. <i>Самостоятельное изучение. Тема 4.</i> Изучение защищенных сетевых протоколов. Изучение работы фильтрующих маршрутизаторов и шлюзов сетевого и прикладного уровня.	1	0,25
Реализация методов защиты информации в современных распределенных системах		2	0,5
39	Вопросы безопасности в различных сетях. Защита корпоративных сетей. Обзор средств защиты информации в системах с распределенной обработкой. Модели безопасности основных операционных систем. Алгоритмы аутентификации пользователей. Аутентификация пользователей при удаленном доступе. Протоколы удаленного доступа пользователя к компьютерной системе. Методы и средства защиты информации в сети. <i>Самостоятельное изучение. Тема 5.</i> Изучение реализации защиты доступа в современных СУБД. Изучение реализации защиты доступа в современных ОС.	2	0,5
Итого часов		8	2

4.2 Практические занятия

Учебным планом не предусмотрены.

4.3 Лабораторные работы

Неделя семестра	Тема и содержание лабораторного занятия	Объем часов	В том числе, в интерактивной форме (ИФ)	Виды контроля
2 семестр		20	5	
Введение в защиту информации		8	2	
24	Лабораторная работа №1 Исследование угроз безопасности информационной системе в соответствии с индивидуальным заданием	4	1	Демонстрация на компьютере. Отчет.
26	Лабораторная работа № 2. Знакомство с эмулятором VirtualBox. Выполнение индивидуальных заданий в среде эмулятора.	4	1	Демонстрация на компьютере. Отчет.
Основы криптографии		4	1	

28	Лабораторная работа № 3. Разработка программы шифрования на основе симметричного ключа. Подготовка отчета	4	1	Демонстрация на компьютере. Отчет.
Реализация методов защиты информации в современных распределенных системах		8	2	
32	Лабораторная работа № 4. Перехват сетевого трафика с помощью программы WireShark. Подготовка отчета.	2	1	Демонстрация на компьютере. Отчет.
36	Лабораторная работа № 5. Работа с сетевым сканером NMap. Подготовка отчета.	2	0,5	Демонстрация на компьютере. Отчет.
38	Лабораторная работа № 6. Настройка брандмауэра Windows и UbuntuLinux. Подготовка отчета.	4	0,5	Демонстрация на компьютере. Отчет.
Итого часов		20	5	

4.4 Самостоятельная работа студента (СРС)

Неделя семестра	Содержание СРС	Объем часов	Виды контроля
2 семестр		80	
23,24	Подготовка в выполнении лабораторной работы №1	4	Допуск
	Работа с конспектом лекций и литературой по теме	4	Опрос
25,26	Подготовка в выполнении лабораторной работы №2	4	Допуск
	Работа с конспектом лекций и литературой по теме	4	Опрос
27,28	Подготовка в выполнении лабораторной работы №3	4	Допуск
	Работа с конспектом лекций и литературой по теме	4	Опрос
29	Изучение примеров атак на информационные системы	4	Опрос
30	Изучение реализаций алгоритмов шифрования с открытым ключом	4	Опрос
31,32	Подготовка в выполнении лабораторной работы № 4	4	Допуск
	Работа с конспектом лекций и литературой по теме	4	Опрос
33	Изучение работы фильтрующих маршрутизаторов и шлюзов сетевого и прикладного уровня.	6	Опрос
34	Изучение защищенных сетевых протоколов.	6	Опрос
35,36	Подготовка в выполнении лабораторной работы № 5	4	Отчет
	Работа с конспектом лекций и литературой по теме	4	Опрос
37	Подготовка в выполнении лабораторной работы № 6	4	Отчет
	Работа с конспектом лекций и литературой по теме	4	Опрос
38	Изучение реализации защиты доступа в современных ОС	6	Опрос
39	Изучение реализации защиты доступа в современных СУБД	6	Опрос
Итого часов		80	

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	В рамках изучения дисциплины предусмотрены следующие образовательные технологии:
5.1	информационные лекции; совместное обсуждение вопросов лекций; подготовка обзоров по темам лекций с одинаковой тематикой разными студентами; дискуссии по проблемным вопросам организации защиты системы распределенной обработки данных.
5.2	лабораторные работы: <ul style="list-style-type: none"> – работа в команде - совместное обсуждение теоретических вопросов выполнения лабораторных заданий, администрирования средств защиты сетевой базы данных, технологий реализации защиты информации в распределенных системах; – программирование специальных функций по защите информации; – индивидуальные задания.
5.3	самостоятельная работа студентов: <ul style="list-style-type: none"> – изучение теоретического материала с использованием Интернет-ресурсов и методических разработок; – подготовка к лекциям и практическим занятиям; – подготовка к лабораторным работам; – работа с учебно-методической литературой; – оформление конспектов лекций, подготовка отчетов по практическим и лабораторным работам; – закрепление теоретического материала при проведении лабораторных работ с использованием учебного оборудования и программного обеспечения; – творческая проблемно-ориентированная самостоятельная работа, ориентированная на развитие общекультурных и профессиональных компетенций, повышение творческого потенциала студентов путем выполнения индивидуальных практических заданий в рамках области исследования; – подготовка к зачету.
5.4	консультации по всем вопросам учебной программы.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6.1	Контрольные вопросы и задания
6.1.1	Используемые формы текущего контроля: <ul style="list-style-type: none"> – опрос, – доклады и презентации по теоретическим темам, – отчеты по практическим и лабораторным работам, – демонстрация навыков работы в изученных системах.
6.1.2	Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения текущего контроля и промежуточной аттестации. Фонд включает вопросы к зачету, тесты.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

№	Авторы, составители	Заглавие	Год изда- ния, вид издания.	Обес- печен- ность
7.1.1 Основная литература				
7.1.1.1	Локшин М.В.	Защита информации в распределенных вычислительных системах: учеб. пособие. - Воронеж: ВГТУ	2014 Электр. Ресурс	1
7.1.2 Дополнительная литература				
7.1.2.1	Кравец О.Я.	Сети ЭВМ и телекоммуникации: учеб. пособие. – Воронеж: «Научная книга»	2010 Печ.	1
7.1.3. Методические разработки				
7.1.3.1	Матвеев Б.В.	Защита информации в телекоммуникационных системах: учеб. пособие. - Воронеж: ВГТУ.	2007 Печ.	1
7.1.3.2	Матвеев Б.В., Душкин А.В.	Защита информации в каналах связи: Лабораторный практикум: Учеб. пособие. - Воронеж: ВГТУ.	2008 Печ.	1
7.1.4 Программное обеспечение и интернет ресурсы				
7.1.3.1	Методические указания к выполнению лабораторных работ и учебные пособия представлены на сетевом диске локальной сети кафедры. Для выполнения лабораторных работ в лабораториях кафедры установлены пакеты программ MSVisualStudio, VirtualBox, WireShark, NMap.			

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	Лекции: специализированная лекционная аудитория, оснащенная доской, учебными столами и проекционной аппаратурой.
8.2	Практические занятия: специализированное помещение для проведения практических занятий, оборудованное доской, учебными столами, проекционной аппаратурой и компьютерами.
8.3	Лабораторные работы: специализированная лаборатория, оборудованная персональными компьютерами с соответствующим программным обеспечением.