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)
30 06 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации
(наименование дисциплины по УП)

Закреплена за кафедрой: Систем автоматизированного проектирования и информационных систем

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

Профили: Вычислительные машины, комплексы, системы и сети, Системы автоматизированного проектирования, Системы автоматизированного проектирования в машиностроении
(название профиля по УП)

Часов по УП: 144; **Часов по РПД:** 144;
Часов по УП (без учета часов на экзамены): 108; **Часов по РПД:** 108;
Часов на самостоятельную работу по УП: 18 (17%);
Часов на самостоятельную работу по РПД: 18 (17%)
Общая трудоемкость в ЗЕТ: 4;
Виды контроля в семестрах (на курсах): Экзамены - 6; Зачет - 0; Зачет с оценкой – 0; Курсовые проекты - 0; Курсовые 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 / 10		Итого	
	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД	УП	РПД
Лекции											36	36					36	36
Лабораторные											54	54					54	54
Практические																		
Ауд. занятия											90	90					90	90
Сам. работа											18	18					18	18
Итого											108	108					108	108

Сведения о ФГОС, в соответствии с которым разработана рабочая программа дисциплины – 09.03.01 «Информатика и вычислительная техника», утвержден приказом Министерства образования и науки Российской Федерации от 12.01.2016 № 5.

Программу составил: _____ к.т.н. Питтолин А. В.
(подпись, ученая степень, ФИО)

Рецензент (ы): _____ к. т. н. Пребенникова Н. Г.
(подпись, ученая степень, ФИО)

Рабочая программа дисциплины составлена на основании учебного плана подготовки бакалавров по направлению 09.03.01 Информатика и вычислительная техника, профиль Системы автоматизированного проектирования.

Рабочая программа обсуждена на заседании кафедры систем автоматизированного проектирования и информационных систем

Зав. кафедрой САПРИС _____ Я.Е. Львович

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	**Цель изучения дисциплины** – Целью преподавания дисциплины «Информационная безопасность» является приобретение студентами теоретических знаний и практических навыков в области защиты информации и информационной безопасности; ознакомление студентов с современными системами информационной безопасности, технологическими приемами защиты информации; возможностями использования средств информационной безопасности при работе с информационными ресурсами
1.2	**Для достижения цели ставятся задачи:**
1.2.1	изучение теоретических основ, методов и средств организационно-правового и технического обеспечения защиты конфиденциальной информации и персональных данных
1.2.2	получение знаний и навыков в области оценки защищенности информации в автоматизированных системах
1.2.3	освоение и использование в практической деятельности технологий информационной безопасности на основе применения специализированных аппаратных и программных средств

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Цикл (раздел) ОПОП: Б1	код дисциплины в УП: Б1.В.ОД.21
2.1 Требования к предварительной подготовке обучающегося	
Для успешного освоения дисциплины студент должен иметь базовую подготовку по информатике, программированию, математике	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее	
Б1.В.ДВ.3.1	Проектирование автоматизированных систем управления
Б1.В.ДВ.7.1	Автоматизация проектирования мобильных беспроводных сетей связи

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-1	способность инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем
ОПК-5	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-3	способностью обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности

В результате освоения дисциплины обучающейся должен

ОПК-1	
3.1	**Знать:**
3.1.1	сущность и понятие информационной безопасности, характеристику ее составляющих
3.1.2	источники угроз информационной безопасности и меры по их предотвращению
3.1.3	жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи

3.1.4	методику применения нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами
3.2	**Уметь:**
3.2.1	пользоваться средствами защиты информации при эксплуатации вычислительной техники, периферийных и мобильных устройств, других технических средств информатизации
3.2.2.	анализировать структурные схемы и порядок взаимодействия компонентов современных технических средств информатизации с точки зрения защиты информации и информационной безопасности
3.2.3	практический опыт мониторинга эффективности программно-аппаратных средств обеспечения информационной безопасности
3.2.4	производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав подсистемы безопасности автоматизированной системы
3.3	**Владеть:**
3.3.1	принципами и методами организационной защиты информации, мерами организационного обеспечения информационной безопасности в организации
3.3.2.	основными нормативными правовыми актами в области информационной безопасности и защиты информации
3.3.3	приемами оформления документации по регламентации мероприятий и оказанию услуг в области защиты информации
3.3.4	приемами установки компонентов подсистемы безопасности в составе автоматизированных информационных систем
ОПК-5	
3.1	**Знать:**
3.1.1	пути решения частных технических задач, возникающих при аттестации объектов, помещений, программ, алгоритмов
3.1.2	оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности
3.1.3	криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись
3.1.4	физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации
3.1.5	номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам
3.2	**Уметь:**
3.2.1	эксплуатировать компоненты подсистем безопасности автоматизированных систем
3.2.2	применять программно-аппаратные средства обеспечения информационной безопасности
3.2.3	использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам
3.2.4	использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения
3.3	**Владеть:**
3.3.1	методами расчета основных характеристик систем экранирования электромагнитных полей, акустической и виброакустической защиты
3.3.2	приемами диагностики, устранения отказов и восстановления работоспособности программно-аппаратных средств обеспечения информационной безопасности
3.3.3	современными средствами и методы построения комплексных систем обеспечения информационной безопасности в автоматизированных системах

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ П./п	Наименование раздела дисциплины	Семестр	Неделя семестра	Вид учебной нагрузки и их трудоемкость в часах				
				Лекции	Практические занятия	Лабораторные. работы	СРС	Всего часов
6 семестр								
1	Понятие информационной безопасности. Основные концептуальные положения системы защиты информации		1-2	4		4	2	10
2	Угрозы конфиденциальной информации. Действия, приводящие к неправомерному овладению конфиденциальной информацией		3-4	4		4	2	10
3	Направления обеспечения информационной безопасности		5-6	4		4	2	10
4	Защита информации от несанкционированного доступа		7-8	4		12	2	18
5	Криптографические средства защиты информации		9-10	4		12	2	18
6	Стандарты и спецификации в области информационной безопасности		11-12	4		6	2	12
7	Информационная безопасность в компьютерных сетях		13-14	4		4	2	10
8	Классификация удаленных угроз в вычислительных сетях		15-16	4		4	2	10
9	Компьютерные вирусы как угроза информационной безопасности. Антивирусные программы, особенности их функционирования и классификация		17-18	4		4	2	10
Итого				36		54	18	108

4.1 Лекции

Неделя семестра	Тема и содержание лекции	Объем часов	В том числе, в интерактивной форме (ИФ)
6 семестр		**36**	
1	Понятие информационной безопасности. Основные определения. Основные концептуальные положения системы защиты информации	2	
2	Модель системы безопасности. Угрозы конфиденциальной информации. Классификация угроз	2	
3	Действия, приводящие к неправомерному овладению конфиденциальной информацией.	2	
4	Направления обеспечения информационной безопасности	2	
5	Организационная защита. Правовые основы информационной безопасности. Инженерно-техническая защита	2	
6	Физические средства защиты Аппаратные средства защиты	2	
7	Программные средства защиты. Основные направления использования программной защиты информации	2	
8	Защита информации от несанкционированного доступа	2	
9-10	Криптографические средства защиты. Общая технология шифрования	4	
11	Защита информации от утечки по техническим каналам. Структура канала утечки информации. Классификация каналов утечки информации	2	
12	Стандарты и спецификации в области информационной безопасности. Стандарт «Критерии оценки доверенных компьютерных систем». Механизмы безопасности. Классы безопасности	2	
13-14	Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Стандарт ISO/IEC «Критерии оценки безопасности информационных технологий». Основные понятия.	4	
15	Информационная безопасность в компьютерных сетях. Распределение функций безопасности по уровням модели	2	
16	Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристики	2	
17-18	Компьютерные вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Антивирусные программы. Особенности функционирования и классификация	4	
Итого часов		**36**	

4.3 Лабораторные работы

Неделя семестра	Наименование лабораторной работы	Объем часов	В том числе в интерактивной форме (ИФ)	Виды контроля
6 семестр		**54**		отчет
2-3	Антивирусная защита информации. Работа с антивирусными пакетами.	6		отчет
4-5	Поточные шифры. Моделирование работы 8-ми (16-ти) разрядного скремблера	6		отчет
6-7	Программная реализация комбинированных криптографических алгоритмов	6		отчет
8-9	Программирование арифметических алгоритмов	6		отчет
10-11	Программирование алгоритмов криптосистем с открытым ключом. Алгоритм шифрации двойным квадратом. Шифр Enigma.	12		отчет
12-13	Алгоритмы шифрования DES и ГОСТ 28147-89.	6		отчет
14-15	Алгоритм шифрования RSA	6		отчет
16-17	Алгоритм шифрования Эль Гамаля. Задачи и алгоритмы электронной подписи.	6		отчет

4.4 Самостоятельная работа студента (СРС)

Неделя семестра	Содержание СРС	Виды контроля	Объем часов
6 семестр			**18**
1-2	Классификация компьютерных преступлений. Личностные особенности компьютерного преступника	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	защита	1
3-4	Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мыши	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	защита	1
5-6	Европейские критерии безопасности информационных технологий. Руководящие документы Гостехкомиссии России	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	защита	1
7-8	Аппаратные средства защиты. Отказоустойчивые дисковые массивы. Источники бесперебойного питания	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	Защита	1

9-10	Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мыши	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	Защита	1
11-12	Аутентификация пользователей при удаленном доступе	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	Защита	1
13-14	Криптосистемы на основе эллиптических уравнений	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	Защита	1
15-16	Методы аналитических преобразований	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	Защита	1
17-18	Криптосистема Эль-Гамаля	Опрос по темам для самостоятельного изучения	1
	Подготовка отчета по выполнению лабораторной работы	Защита	1

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

	В рамках изучения дисциплины предусмотрены следующие образовательные технологии:
5.1	**Информационные лекции**
5.2	**лабораторные работы**: – выполнение лабораторных работ в соответствии с индивидуальным графиком, – защита выполненных работ;
5.4	**самостоятельная работа студентов**: – изучение теоретического материала, – подготовка к лекциям, лабораторным работам, – работа с учебно-методической литературой, – оформление конспектов лекций, подготовка отчетов, – подготовка к текущему контролю, экзамену
5.5	**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:

	– отчет и защита выполненных лабораторных работ.
6.1.2	Рабочая программа дисциплины обеспечена фондом оценочных средств для проведения контроля. Фонд включает вопросы к экзамену, тестовые задания. Фонд оценочных средств, представлен в учебно–методическом комплексе дисциплины.

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

7.1 Рекомендуемая литература				
№ п/п	Авторы, составители	Заглавие	Годы издания. Вид издания	Обеспеченность
7.1.1. Основная литература				
7.1.1.1	**Мельников В.П.**	Информационная безопасность : Учеб. пособие / под ред. С. А. Клейменова. - 8-е изд., испр. - М. : Академия, 2013. - 336	2013 печ.	
7.1.1.2	**Малюк А.А.**	Информационная безопасность : концептуальные и методологические основы защиты информации : Учеб. пособие. - М. : Горячая линия -Телеком, 2004. - 280 с.	2004 печ.	
7.1.2. Дополнительная литература				
7.1.2.1	**Паринов А.В.**	Информационная безопасность и защита информации [Электронный ресурс] : Учеб. пособие. - Электрон. дан. (1 файл : 811 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007.	2007 магн.	
7.1.2.2	**Кольцов А.С.**	Информационная безопасность и защита информации [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (4,5 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013	2013 магн.	
7.1.3 Методическая литература				
7.1.3.1	**Чопоров О.Н.**	Защита информации и информационная безопасность [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (1,8 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012.	2012 магн.	
7.1.3.2.	**Локшин М.В.**	Защита информации в распределенных вычислительных системах [Электронный ресурс] . - Электрон. текстовые, граф. дан. (1262 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2014.	2014 магн.	

7.2 Программное обеспечение и интернет ресурсы	
7.2.1	1. www.citforum.ru, 2. www.intuit.ru
7.2.2	**Компьютерные лабораторные работы**: – C++, Delphi 7.0

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	**Специализированная лекционная аудитория**
8.2	**Дисплейный класс**, оснащенный компьютерными программами для проведения лабораторного практикума