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)
17 06 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

(наименование дисциплины по УП)

Закреплена за кафедрой: Систем автоматизированного проектирования и информационных систем

Направление подготовки (специальности):
09.03.02 Информационные системы и технологии
(код, наименование)

Профиль: Информационные системы и технологии
(название профиля по УП)

Часов по УП: 216**; Часов по РПД:** 216;
Часов по УП (без учета часов на экзамены): 180**; Часов по РПД:** 180**;**
Часов на самостоятельную работу по УП: 72 (40 %);
Часов на самостоятельную работу по РПД: 72 (40 %);
Общая трудоемкость в ЗЕТ: 6;
Виды контроля в семестрах: Экзамены - 7; Зачеты – 6; Зачеты с оценкой – 0; Курсовые проекты -0; Курсовые работы - 7.
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											36	36	18	18			54	54
Лабораторные											18	18	36	36			54	54
Практические																		
Ауд. занятия											54	54	54	54			108	108
Сам. работа											54	54	18	18			72	72
Итого											108	108	72	72			180	180

Сведения о ФГОС, в соответствии с которым разработана рабочая программа дисциплины – 09.03.02 «Информационные системы и технологии», утвержден приказом Министерства образования и науки Российской Федерации 12 марта 2015 № 219.

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

Рецензент (ы): _____ к.т.н. Сидоров В.В.
(подпись, ученая степень, ФИО)

Рабочая программа дисциплины составлена на основании учебного плана подготовки бакалавров по направлению 09.03.02 Информационные системы и технологии, профиль Информационные системы и технологии

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

протокол № 13 от 06.06 2016 г.

Зав. кафедрой САПРИС _____ Я.Е. Львович

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	**Цель изучения дисциплины** – Целью преподавания дисциплины «Информационная безопасность и защита информации» 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 ООП ВО

Цикл (раздел) ООП: Б1	код дисциплины в УП: Б1.В.ОД.4
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.ОД.10	Администрирование серверов баз данных

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-4	понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны
ПВК-5	способность обеспечивать работоспособность и надежность информационных систем в заданных функциональных характеристиках
ПВК- 6	способность использовать методы обеспечения безопасности и целостности данных информационных систем и технологий
ПВК-7	способность адаптировать приложения к изменяющимся условиям функционирования

В результате освоения дисциплины обучающейся должен

ОПК-4	понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны
3.1	**Знать:**
3.1.1	основные теоретические положения функционирования и развития систем информационной безопасности, основные направления обеспечения информационной безопасности
3.3	**Владеть:**
3.3.1.	методами и средствами защиты информации в информационно - телекоммуникационных системах
ПВК-5	способность обеспечивать работоспособность и надежность информационных систем в заданных функциональных характеристиках
3.1	**Знать:**
3.1.1	угрозы информации и информационным технологиям в информационно-телекоммуникационных системах
3.2	**Уметь:**
3.2.1	проводить анализ потенциально возможных угроз информации и информационным технологиям в компьютерных системах
ПВК-6	способность использовать методы обеспечения безопасности и целостности данных информационных систем и технологий
3.1	**Знать:**
3.1.1	способы и средства защиты информации от несанкционированного доступа в технических каналах связи информационно-телекоммуникационных систем
3.2	**Уметь:**
3.2.1	проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем
ПВК-7	способность адаптировать приложения к изменяющимся условиям функционирования
3.1.	**Знать:**
3.1.1.	стандарты в области информационной безопасности
3.2	**Уметь:**
3.2.1.	инсталлировать тестировать и использовать программные компоненты информационных систем, ориентированные на решение задач защиты информации и обеспечение информационной безопасности
3.3.	**Владеть:**
3.3.1.	навыками работы с программными и аппаратными средствами, применяемыми в области информационной безопасности и защиты информации

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	8
2	Угрозы конфиденциальной информации. Действия, приводящие к неправомерному овладению конфиденциальной информацией		3-4	6		2	6	14
3	Направления обеспечения информационной безопасности		5-6	4		4	10	18
4	Защита информации от несанкционированного доступа		7-11	8		4	6	18
5	Криптографические средства защиты информации		12-15	8		8	16	32
6	Стандарты и спецификации в области информационной безопасности		16-18	6			12	18
7 семестр								
7	Информационная безопасность в компьютерных сетях		1-6	6		12	6	24
8	Удаленные угрозы в вычислительных сетях		7-14	8		16	6	30
9	Компьютерные вирусы как угроза информационной безопасности. Антивирусные программы, особенности их функционирования и классификация		15-18	4		8	6	18
Итого				54		54	72	180

4.1 Лекции

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

5-6	Классификация удаленных угроз в вычислительных сетях.	2	
7-10	Типовые удаленные атаки и их характеристики	4	
11-12	Компьютерные вирусы как угроза информационной безопасности.	2	
13-16	Классификация компьютерных вирусов.	4	
17-18	Антивирусные программы. Особенности функционирования и классификация	2	
Итого часов		**54**	

4.3 Лабораторные работы

Неделя семестра	Наименование лабораторной работы	Объем часов	В том числе в интерактивной форме (ИФ)	Виды контроля
6 семестр		**18**		отчет
1-8	Антивирусная защита информации. Работа с антивирусными пакетами.	8		отчет
8-16	Поточные шифры. Моделирование работы 8-ми (16-ти) разрядного скремблера	10		отчет
7 семестр		**36**		
1-4	Программная реализация комбинированных криптографических алгоритмов	8		отчет
5-6	Программирование арифметических алгоритмов	4		отчет
7-10	Программирование алгоритмов криптосистем с открытым ключом. Алгоритм шифрации двойным квадратом. Шифр Enigma.	8		отчет
11-12	Алгоритмы шифрования DES и ГОСТ 28147-89.	4		отчет
13-14	Алгоритм шифрования RSA	4		отчет
15-18	Алгоритм шифрования Эль Гамаля. Задачи и алгоритмы электронной подписи.	8		отчет

4.4 Самостоятельная работа студента (СРС)

Неделя семестра	Содержание СРС	Виды контроля	Объем часов
6 семестр			**54**
1-4	Классификация компьютерных преступлений. Личностные особенности компьютерного преступника	Опрос по темам для самостоятельного изучения	6
	Подготовка отчета по выполнению лабораторной работы	защита	4

5-8	Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мыши	Опрос по темам для самостоятельного изучения	6
	Подготовка отчета по выполнению лабораторной работы	защита	4
9-12	Европейские критерии безопасности информационных технологий. Руководящие документы Гостехкомиссии России	Опрос по темам для самостоятельного изучения	6
	Подготовка отчета по выполнению лабораторной работы	защита	2
13-16	Аппаратные средства защиты. Отказоустойчивые дисковые массивы. Источники бесперебойного питания	Опрос по темам для самостоятельного изучения	6
	Подготовка отчета по выполнению лабораторной работы	Защита	2
17-18	Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мыши	Опрос по темам для самостоятельного изучения	6
	Подготовка отчета по выполнению лабораторной работы	Защита	4
7 семестр			**18**
1-4	Аутентификация пользователей при удаленном доступе	Опрос по темам для самостоятельного изучения	2
	Подготовка отчета по выполнению лабораторной работы	Защита	1
	Курсовое проектирование	Консультация	1
5-8	Криптосистемы на основе эллиптических уравнений	Опрос по темам для самостоятельного изучения	2
	Курсовое проектирование	Консультация	1
	Подготовка отчета по выполнению лабораторной работы	Защита	1
9-12	Методы аналитических преобразований	Опрос по темам для самостоятельного изучения	2
	Курсовое проектирование	Консультация	2
	Подготовка отчета по выполнению лабораторной работы	Защита	1
13-18	Криптосистема Эль-Гамаля	Опрос по темам для самостоятельного изучения	2
	Курсовое проектирование	Консультация	2
	Подготовка отчета по выполнению лабораторной работы	Защита	1

Итого			**72**

4.5. Курсовое проектирование

Целью курсового проекта по дисциплине «Информационная безопасность и защита информации» является закрепление теоретического материала и практических навыков, полученных студентами при изучении дисциплины.

В процессе выполнения курсового проекта студент должен:

- закрепить, углубить и расширить теоретические знания о предметной области дисциплины;
- овладеть навыками самостоятельной работы по направлениям деятельности изучаемой дисциплины;
- выработать умения формулировать суждения и выводы, логически последовательно и доказательно их излагать;
- выработать навык публичной защиты;
- подготовиться к более сложной задаче -- выполнение дипломной работы.

Примерная тематика курсового проектирования

1. Шифры замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат.
2. Шифры замены Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.
3. Шифры гаммирования. Шифр Вернама.
4. Композиции шифров. Enigma. Шифр Хейглина.
5. Блочные шифры и их ключевая система. Сеть Файстеля.
6. Шифр ГОСТ 28147-89.
7. Криптографические хэш-функции. Хэш-функции на основе блочного шифра.
8. Криптосистема Диффи-Хэллмана.
9. Криптосистема RSA.
10. Криптосистема Эль-Гамаля.
11. Криптосистема Рабина.
12. Криптосистема Гольдвассер-Микали.
13. Криптосистема Блюма-Гольдвассер.
14. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
15. Режимы шифрования. Многократное шифрование. Композиция блочных шифров
16. Поточные шифры. Синхронные и самосинхронизирующиеся шифры
17. Поточные фильтры. Скремблирование
18. Блочный шифр AES
19. Криптосистемы на эллиптических кривых

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, зачету
5.5	**консультации** по всем вопросам учебной программы.

Методические указания для студентов по освоению дисциплины

Система университетского образования предполагает рациональное сочетание таких видов учебной деятельности, как лекции, лабораторные работы, самостоятельная работа студентов, а также контроль полученных знаний.

- Лекции представляет собой систематическое, последовательное изложение учебного материала. Это – одна из важнейших форм учебного процесса и один из основных методов преподавания в вузе. На лекциях от студента требуется не просто внимание, но и самостоятельное оформление конспекта. В качестве ценного совета рекомендуется записывать не каждое слово лектора (иначе можно потерять мысль и начать писать автоматически, не вникая в смысл), а постараться понять основную мысль лектора, а затем записать, используя понятные сокращения.

- Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных работ для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, проработать дополнительную литературу и источники. - Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие:

- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;

- работа над темами для самостоятельного изучения;

- участие в работе студенческих научных конференций, олимпиад;

- подготовка к зачетам и экзаменам.

Кроме базовых учебников рекомендуется самостоятельно использовать имеющиеся в библиотеке учебно-методические пособия. Независимо от вида учебника, работа с ним должна происходить в течение всего семестра. Эффективнее работать с учебником не после, а перед лекцией.

Степень усвоения материала проверяется следующими видами контроля:

- текущий (опрос, контрольные работы);

- защита лабораторных работ;

- промежуточный (курсовая работа, зачет, зачет, экзамен).

Коллоквиум – форма итоговой проверки знаний студентов по определенным темам.

Зачет – форма проверки знаний и навыков, полученных на лекционных и лабораторных занятиях. Сдача всех зачетов, предусмотренных учебным планом на данный семестр, является обязательным условием для допуска к экзаменационной сессии.

Экзамен – форма итоговой проверки знаний студентов.

Для успешной сдачи экзамена необходимо выполнить следующие рекомендации – готовиться к экзамену следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до экзамена. Данные перед экзаменом три-четыре дня эффективнее всего использовать для повторения и систематизации материала.

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 зачету. Фонд оценочных средств, представлен в учебно–методическом комплексе дисциплины.

6.1. Формы текущего контроля

Раздел дисциплины	Объект контроля	Форма контроля	Метод контроля	Срок выполнения
6 семестр				
Основные концептуальные положения системы защиты информации	Знание основных понятий и определений в области информационной безопасности и защиты информации	Лабораторная работа	Защита лабораторной работы	2 неделя
Угрозы конфиденциальной информации.	Знание классификации угроз, моделей угроз информационной безопасности	Лабораторная работа	Защита лабораторной работы	4 неделя
Направления обеспечения информационной безопасности	Знание направлений обеспечения информационной безопасности	Контрольная работа	Письменный опрос	6 неделя
Защита информации от несанкционированного доступа	Владение методами идентификации, аутентификации, парольной защиты	Лабораторная работа	Защита лабораторной работы	8 неделя
Криптографические средства защиты информации	Умение разрабатывать программные реализации криптографических алгоритмов	Лабораторная работа	Защита лабораторной работы	10 неделя
Стандарты и спецификации в области информационной безопасности	Знание российских стандартов и международных стандартов и спецификаций	Контрольная работа	Письменный опрос	12 неделя
Промежуточная аттестация		зачет	Устный опрос	14 неделя
Основные концептуальные положения системы защиты информации; угрозы конфиденциальной информации; направления обеспечения	Знание основных понятий и определений в области информационной			

информационной безопасности; защита информации от несанкционированного доступа; криптографические средства защиты информации; стандарты и спецификации в области информационной безопасности;	безопасности и защиты информации; Знание классификации угроз, моделей угроз информационной безопасности;			
7 семестр				
Информационная безопасность в компьютерных сетях	Знание классификации удаленных угроз в вычислительных сетях; Уметь эксплуатировать компоненты подсистем безопасности автоматизированных систем	Лабораторная работа	Защита лабораторной работы	4 неделя
Компьютерные вирусы как угроза информационной безопасности. Антивирусные программы, особенности их функционирования и классификация	Уметь пользоваться средствами антивирусной защиты информации при эксплуатации вычислительной техники,	Лабораторная работа	Защита лабораторной работы	8 неделя
Промежуточная аттестация				
информационная безопасность в компьютерных сетях; компьютерные вирусы как угроза информационной безопасности. Антивирусные программы, особенности их функционирования и классификация	Знание российских стандартов и международных стандартов и спецификаций; Знание классификации удаленных угроз в вычислительных сетях;	экзамен	Устный опрос	18 неделя

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	**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.	1
7.1.1.2	**Прохорова О.В.**	Информационная безопасность и защита информации : учебник - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331	2014	1
7.1.1.3	**Скрипник Д.А.**	Общие вопросы технической защиты информации / - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. : ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070	2016	1
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.	1
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.	1
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.	0,1
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

4.