МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
Воронежский государственный технический университет
(ФГБОУ ВО «ВГТУ», ВГТУ)

УТВЕРЖДАЮ
Декан факультета
«Экономики, менеджмента и
информационных технологий»
С.А. Баркалов
«07» сентября **2017 г.**

РАБОЧАЯ ПРОГРАММА
Дисциплины

«Информационная безопасность и защита информации»

Направление подготовки (специальность) 09.03.02 «Информационные системы и технологии»

Профиль Информационные системы и технологии в строительстве

Квалификация (степень) выпускника бакалавр
Нормативный срок обучения 4 года
Форма обучения очная

Автор программы канд. техн. наук, доцент Здольник В.В.

Программа обсуждена на заседании кафедры «Информационных технологий и автоматизированного проектирования в строительстве»

«31» августа 2017 года Протокол № 1

Зав. кафедрой _____ А.В. Смольянинов

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Цели дисциплины

Целью данной дисциплины является углубленное изучение основополагающих принципов информационной безопасности и защиты информации на современных объектах информатизации. Знакомство студентов и изучение моделей угроз информационной безопасности, терминологией и основными понятиями теории и практики защиты информации, а так же с нормативными правовыми актами как Российской Федерации так и зарубежных стран регламентирующих деятельность в сфере информационной безопасности.

Задачи освоения дисциплины

Задачами преподавания дисциплины являются:

- изучение нормативных правовых актов регламентирующих деятельность в области информационной безопасности и защиты информации;
- изучение современных теоретических, практических и методологических аспектов информационной безопасности и защиты информации;
- изучение современных угроз информационной безопасности, а также концептуальных проблем выявления угроз информационной безопасности;
- изучение основных способов, средств и методов обеспечения информационной безопасности и защиты информации как в условиях обработки информации на объектах информатизации так и в условиях передачи информации по каналам связи;
- приобретения теоретических и практических навыков использования современных средств обеспечения информационной безопасности и защиты информации;
- приобретение теоретических и практических навыков реализации мер защиты информации на объектах информатизации;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП

Дисциплина «Информационная безопасность и защита информации» относится к вариативной части дисциплин блока «Дисциплины (модули)» учебного плана. При ее освоении используется знания, полученные в курсах: Архитектура и администрирование операционных систем, Правоведенье, Телекоммуникационные системы и сети.

Для успешного освоения дисциплины студент должен знать:

– методы и средства администрирования информационных систем;
– архитектуру компьютерных сетей;

Обладать умениями и навыками:

– работы в качестве администратора информационных систем;
– использования внешних носителей информации для обмена данными между персональными компьютерами;
– создания резервных копий и архивов данных;
– анализа структуры обрабатываемых данных в информационных системах.

Знания, полученные при изучении дисциплины «Информационная безопасность и защиты информации» используются в написании ВКР.

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Теоретические знания и практические навыки, полученные обучаемыми при изучении дисциплины, должны быть использованы в процессе изучения последующих дисциплин по учебному плану, при подготовке выпускной квалификационной работы и в последующей профессиональной деятельности.

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование общекультурных и профессиональных компетенций:

- пониманием сущности и значения информации в развитии современного общества, соблюдение основных требований к информационной безопасности, в том числе защиты государственной тайны (ОПК-4);
- способность проводить предпроектное обследование объекта проектирования. системный анализ предметной области, их взаимосвязей (ПК-1);
- способность оценивать надежность и качество функционирования объекта проектирования (ПК-6);
- способность обнаруживать угрозы безопасности и устранять нарушения целостности данных (ДКП-4);

В результате изучения дисциплины студент должен:

Знать:

- концепцию информационной безопасности Российской Федерации и основные нормативные правовые акты в области информационной безопасности и защиты информации;
- основные термины и определения в области информационной безопасности и защиты информации;
- классификацию и характеристики каналов утечки информации;
- классификацию и характеристики основных методов и средств защиты информации;

- способы построения модели угроз информационной безопасности;
- принципы работа с персоналом имеющим доступ к информации ограниченного распространения;
- принципы построения модели угроз информационной безопасности;
- принципы реализации организационных, программных, аппаратных, программно-аппаратных средств защиты информации;

Уметь:

- структурировать информационные ресурсы в соответствии с их ценностью и уровнем конфиденциальности, определять необходимость их защиты от несанкционированного доступа;
- определять направление развития (модернизации) системы защиты информации в соответствии с текущими требованиями нормативно правовых актов регламентирующих деятельность в области защиты информации;
- классифицировать виды угроз информационной безопасности;
- разрабатывать нормативно-методические материалы по регламентации деятельности персонала задействованного как в процессах обработки защищаемой информации так и в процессах направленных на защиту информации;
- анализировать уровень эффективности используемых средств и методов защиты информации;
- анализировать уровень защищенности используемых информационных систем;
- анализировать уровень и качество приобретенных знаний в области обеспечения информационной безопасности и защиты информации;
- применять основополагающие принципы обеспечения информационной безопасности и защиты информации при проектировании информационных систем.

Владеть:

- терминологией в области информационной безопасности и защиты информации;
- навыками классификации угроз информационной безопасности;
- методами системного анализа информационных систем;
- методами системного анализа информационных систем;
- методами построения защищенных информационных систем;
- навыками разработки модели угроз информационной безопасности;

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Информационная безопасность и защиты информации» составляет 5 зачетных единицы.

Вид учебной работы	Всего часов	Семестры			
		8			
Аудиторные занятия (всего)	56/-	56/-	-/-		
В том числе:					
Лекции	28/-	28/-	-/-		
Практические занятия (ПЗ)	-/-	-/-	-/-		
Лабораторные работы (ЛР)	28/-	28/-	-/-		
Самостоятельная работа (всего)	88/-	88/-	-		
В том числе:					
Курсовая работа		36	-		
Контрольная работа	-	-	-		
Подготовка к лабораторным и практическим работам	-	-			
Вид промежуточной аттестации (зачет, экзамен)	36	Экзамен/36	-		
Общая трудоемкость час	180	180	-		
зач. ед.	5	5	-		

Примечание: здесь и далее числитель – очная/знаменатель – заочная формы обучения.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Основы информационной безопасности и защиты информации в современных условия	Нормативные правовые акты регламентирующие деятельность в сфере обеспечения информационной безопасности и защиты информации. Основные термины и определения информационной безопасности и защиты информации. Исторические аспекты развития информационной безопасности как науки. Проблема обеспечения информационной безопасности в Российской Федерации. Требования к защите конфиденциальной и секретной информации. Информационная безопасность как неотъемлемая часть деятельности общества. Классификация современных методов обеспечения информационной безопасности. Системный подход в вопросе обеспечения информационной безопасности и защиты информации на объектах информатизации. Побочные электромагнитные излучения и наводки как канал утечки защищаемой информации.

№ п/п	Наименование раздела дисциплины	Содержание раздела
2	Методы и средства обеспечения информационной безопасности.	Современные системы разграничения доступа к информационным ресурсам. Использование организационно-правовых, технических (аппаратных), программных, программно-аппаратных методов защиты информации. Задачи систем обеспечения информационной безопасности. Разграничение доступа как средство обеспечения защиты информации. Модели разграничения доступа, разделение привилегий на доступ.
3	Криптографические средства обеспечения информационной безопасности	Шифрование как инструмент защиты информации. Криптографические методы и средства обеспечения защиты информации. Использование криптографических средств защиты информации в современных информационных системах.
4	Вредоносное программное обеспечение как угроза информационной безопасности.	Исторические аспекты компьютерных вирусов. Компьютерные вирусы как разновидность вредоносного программного обеспечения в современных условиях. Классификация компьютерных вирусов. Интеграция вредоносного программного обеспечения в мобильных платформах. Методы и способы обнаружения и анализа алгоритма вредоносного программного обеспечения.
5	Реализация мер защиты информации на программном уровне.	Реализация механизмов защиты информации как компонент современных информационных систем. Правовые основы использования механизмов защиты информации в современных информационных системах. Исследование программного обеспечения как угроза информационной безопасности. Методы и средства защиты программного обеспечения от исследование. Роль механизмов идентификации и аутентификации в современном программном обеспечении.
6	Вопросы обеспечения защиты информации в распределенных информационных системах.	Особенности формирования каналов утечки информации в распределенных информационных системах. Современные средства и методы анализа состояния защищенности распределенных информационных систем. Проблемы обеспечения информационной безопасности в современных распределенных информационных системах. Аспекты разработки модели угроз распределенной информационной системы.

5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

Дисциплина "Информационная безопасности и защита информации" необходима при написании студентами выпускной квалификационной работы.

5.3. Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Практ. зан.	Лаб. зан.	СРС	Все-го час.
1.	Основы информационную безопасность и защиты информации в современных условия	6		6	20	32
2.	Методы и средства обеспечения информационной безопасности.	4		4	12	20
3.	Криптографические средства обеспечения информационной безопасности	4		4	12	20
4.	Вредоносное программное обеспечение как угроза информационной безопасности..	4		4	12	20
5.	Реализация мер защиты информации на программном уровне.	6		6	20	32
6.	Вопросы обеспечения защиты информации в распределенных информационных системах.	4		4	12	20

5.4. Лабораторный практикум

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Трудоемкость (час)
1.	2,4,5,6	Возможности разграничения доступа к информационным ресурсам в современных серверных операционных системах. Анализ возможностей администрирования, разграничения и контроля доступа к информационным ресурсам в современных информационных системах. Реализация ограничения доступа в пользовательских приложениях. Архивирование данных как средство обеспечения информационной безопасности. Вопросы администрирования антивирусного программного обеспечения.	6
2.	2,3,4,5,6	Организация идентификации и аутентификации пользователей инструментами серверных операционных систем. Обеспечение парольной защиты в пользовательских приложениях. Эффективность парольной защиты современных архиваторов. Эффективность парольной защиты электронных документов.	4
3.	2,4,6	Восстановления информации на носителях информации различного типа.	4
4.	2,3	Использование стандартных инструментов серверных операционных систем при создании виртуальных каналов передачи информации. Использование криптографических протоколов передачи информации.	4
5.	2,3,4,5,6	Современные механизмы защиты программ от ис-	6

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Трудоемкость (час)
		следования. Дизассемблирование и трассировка. Обнаружение и удаление вредоносного программного обеспечения. Администрирование современных средств сетевой безопасности.	
6.	6	Разработка модели угроз	4

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ И КОНТРОЛЬНЫХ РАБОТ

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.

Типовая структура курсового проекта следующая:

1. Титульный лист, введение;
2. Формулировка задания;
3. Основная часть;
4. Заключение;
5. Список литературы;
6. Приложения.

Примерные темы курсовых проектов:

1. Правовые основы организации информационной безопасности на объектах информатизации.
2. Каналы утечки информации как угроза информационной безопасности.
3. Защита информации от утечек по техническим каналам
4. Персональные данные как объект защиты информации.
5. Модель угроз как компонент современной системы защиты информации.
6. Системный подход в вопросе обеспечения информационной безо-

пасности на объектах информатизации.

7. Современные каналы утечки информации и способы защиты информации.

8. Основные и вспомогательные технические средства связи.

9. Использование программных средств защиты информации в современных информационных системах.

10. Использование программно-аппаратных комплексов защиты информации в современных условиях.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

№ п/п	Компетенция (общепрофессиональная ОПК, профессиональная – ПК, дополнительная профессиональная -ДПК)	Форма контроля	Семестр
1.	пониманием сущности и значения информации в развитии современного общества, соблюдение основных требований к информационной безопасности, в том числе защиты государственной тайны (ОПК-4)	Защита лабораторных работ (ЗЛР) Экзамен (Э) Защита курсового проекта (КП)	8
2.	способность проводить предпроектное обследование объекта проектирования, системный анализ предметной области, их взаимосвязей (ПК-1)	Защита курсового проекта (КП)	8
3.	способность оценивать надежность и качество функционирования объекта проектирования (ПК-6)	Реферат (Р) Защита лабораторных работ (ЗЛР) Экзамен (Э) Защита курсового проекта (КП) Тестирование (Т)	8
4.	способность обнаруживать угрозы безопасности и устранять нарушения целостности данных (ДПК-4)	Реферат (Р) Защита лабораторных работ (ЗЛР) Экзамен (Э) Защита курсового проекта (КП) Тестирование (Т)	8

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Дескриптор компетенции	Показатель оценивания	Форма контроля					
		КП	ЗПР	Р	ЗЛР	Т	Экз.
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и на-	+		+		+	+

Дескриптор компетенции	Показатель оценивания	Форма контроля					
		КП	ЗПР	Р	ЗЛР	Т	Экз.
	водки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)						
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)	+		+	+	+	+
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных опера-	+		+	+	+	+

Дескриптор компетенции	Показатель оценивания	Форма контроля					
		КП	ЗПР	Р	ЗЛР	Т	Экз.
	ционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)						

7.2.1. Этап текущего контроля знаний

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по пятибалльной шкале с оценками:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «неудовлетворительно»;
- «не аттестован».

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)	отлично	Полное или частичное посещение лекционных, лабораторных занятий. Защита лабораторных работ на отлично. Выполненные КП и Р на оценку «отлично».
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты.		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)	хорошо	Полное или частичное посещение лекционных, лабораторных занятий. Защита лабораторных работ на отлично и хорошо. Выполненные КП и Р на оценку «хорошо».
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)	удовлетворительно	Полное или частичное посещение лекционных, лабораторных занятий. Защита лабораторных работ на удовлетворительно. Удовлетворительно выполненные КП и Р

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основ-	неудовлетворительно	Частичное посещение лекционных, лабораторных занятий. Защита лабораторных работ на неудовлетворительно. Неудовлетво-

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	ные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)		рительно выполненные КП и Р
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и	не аттестован	Непосещение лекционных, лабораторных занятий. Нет выполненных и

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)		защищенных лабораторных работ. Не выполнены КП и Р
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		

7.2.2. Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний (экзамен) оцениваются по четырехбалльной шкале с оценками:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «неудовлетворительно»

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)	отлично	Студент демонстрирует полное понимание заданий. Все требования, предъявляемые к заданиям выполнены
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты ин-		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	формации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)	хорошо	Студент демонстрирует значительное понимание заданий. Все требования, предъявляемые к заданиям выполнены
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)	удовлетворительно	Студент демонстрирует частичное понимание заданий. Большинство требований, предъявляемых к заданиям выполнены
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления данных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации.		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Знает	Акустические, акустоэлектрические, виброакустические, оптические, электромагнитные, радиоизлучения и наводки, материальные каналы и утечки информации. состав, структуру, принципы реализации и функционирования систем защиты информации, используемых при создании защищенных информационных систем; принципы организации защиты информации на объектах информатизации. Основные принципы защиты компьютерной информации. Вопросы обеспечения защиты персональных данных в информационных системах персональных данных (ОПК-4, ПК-1, ПК-6, ДПК-4)	неудовлетворительно	1. Студент демонстрирует небольшое понимание заданий. Многие требования, предъявляемые к заданиям не выполнены. 2. Студент демонстрирует непонимание заданий. 3. У студента нет ответа. Не было попытки выполнить задания
Умеет	Осуществлять настройку разграничения прав доступа в современных операционных системах, в том числе серверных операционных системах. Работать с современными программными комплексами реализующих функции по защите информации, в том числе обеспечивающими функции восстановления дан-		

Дескриптор компетенции	Показатель оценивания	Оценка	Критерий оценивания
	ных, архивирования, межсетевого экранирования, антивирусной защиты. Определять актуальные угрозы информационной безопасности на объектах информатизации. Разрабатывать организационно-планирующую документацию в области защиты информации для типового объекта информатизации (ОПК-4, ПК-1, ПК-6, ДПК-4)		
Владеет	навыками классификации каналов утечки информации на объектах информатизации; навыками разработки моделей угроз для информационных систем; навыками организации систем защиты информации для информационных систем персональных данных; навыками администрирования разграничения доступа к информационным ресурсам в информационных системах под управлением современных операционных систем; навыками работы с современными антивирусными программными продуктами; навыками классификации угроз информационной безопасности в том числе в информационных системах персональных данных; (ОПК-4, ПК-1, ПК-6, ДПК-4)		

7.3.Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

Текущий контроль успеваемости осуществляется, на лабораторных занятиях в виде опроса теоретического материла и самостоятельного выполнения практических заданий под контролем преподавателя, а также в виде тестирования по отдельным темам.

Промежуточный контроль осуществляется проведением контрольных точек по отдельным разделам дисциплины, тестирования по разделам дисциплины, изученным студентом в период между аттестациями. Контрольные точки проводятся на лабораторных в рамках самостоятельной работы под контролем преподавателя. Варианты контрольных заданий выдаются каждому студенту индивидуально.

7.3.1. Примерная тематика типовых контрольных заданий

1. Что такое национальные интересы? Какие другие виды интересов вам известны?

2. В чем могут заключаться национальные интересы России? В чем заключается национальная безопасность, ее определения?

3. В чем состоят основные угрозы безопасности России?

4. Что такое информационная безопасность, каковы ее основные аспекты?

5. В чем заключаются жизненно важные интересы в информационной сфере и угрозы жизненно важным интересам в информационной сфере?

6. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации.

7. Что такое информационная война и информационное превосходство?

8. Перечислите методы идентификации и установления подлинности субъектов и различных объектов.

9. Каковы методы своевременного обнаружения несанкционированных действий пользователей?

10. В чем состоят задачи контроля информационной целостности?

11. Перечислите способы определения модификаций информации.

12. Назовите методы регистрации действий пользователей.

13. Объясните суть криптографического преобразования — перестановка и замена.

14. Что из себя представляет симметричная криптографическая система?

15. Объясните суть алгоритма DES и укажите на его особенности. В каких режимах может работать алгоритм DES?

16.Дайте описание отечественного алгоритма криптографического преобразования. Какие режимы имеет отечественный алгоритм криптографического преобразования данных (ГОСТ 28147—90)?

17. Какими характеристиками оценивается стойкость криптографических систем?

18. В чем заключается суть электронной цифровой подписи? Как проверяется целостность сообщения?

19. Что называется открытым ключом и секретным ключом? Какая связь существует между открытыми и секретными ключами? Приведите примеры.

20. Каковы способы заражения программ компьютерными вирусами. Опишите методы и схему функционирования вирусов.

21. Сформулируйте цели защиты информации в сетях ЭВМ и назовите основные угрозы информации в сетях.

22. Приведите перечень основных механизмов защиты информации в сетях и дайте им краткую характеристику.

23. В чем состоят функции средств анализа защищенности компьютерных систем и каковы их основные недостатки?

24. В чем сущность систем обнаружения атак на компьютерные систе-

мы?

25. Какие применяются разновидности межсетевых экранов? Каковы общие недостатки всех межсетевых экранов?.

7.3.2 Примерные задания для тестирования

Таблица 1

Значение термина "Защита информации" определено в Федеральном законе:
Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"
Федеральный закон от 27 июля 2006 г. N **152-ФЗ** "О персональных данных"
Федеральный закон от 27 июля 2006 г. N 159-ФЗ "О защите информации в Российской Федерации"

Таблица 2

Информация – это
сведения (сообщения, данные) независимо от формы их представления
Любые сведения обрабатываемые в информационных системах
Данные об объектах, лицах, независимо от формы их представления.
Персональные данные не зависимо от формы представления.

Таблица3

Авторизация – это:
Предоставление конкретному пользователю к определенным системным ресурсам
Проверка личности пользователя
Идентификация пользователя
Аутентификация пользователя

Таблица 4

К числу основных угроз информационной безопасности не относится:
Защита от копирования
Целостность
Доступность
Конфиденциальность

Таблица 5

Политика информационной безопасности строится на основе:
Анализа рисков
Сбора сведений о персонале
Общих представлений об АИС объекта информатизации
Изучения номенклатуры должностей организации

Таблица 6

Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:
Информационно-телекоммуникационная сеть
Информационная система
База данных
Информационная технология

Таблица 7

Компоненты информационной системы предприятия, в котором накапливаются и обраба-

тываются персональные данные это:
Информационная сеть персональных данных
Система управления базами данных
Хранилище данных
Коммуникационный узел

Таблица 8

Процесс сообщения субъектом своего имени или номера, с целью получения определенных полномочий на выполнение некоторых действий в информационных системах с ограниченным доступом:
Идентификация
Авторизация
Регистрация
Детализация

Таблица 9

Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи информации, в том числе по сети Интернет:
Шифрования
Парольная защита
Авторизация пользователей сети
Экспертиза

Таблица 10

Несанкционированный доступ к информации – это:
Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
Вход в информационную систему без регистрации пользователя
Доступ к информационным ресурсам от имени другого пользователя
Доступ к информационным ресурсам, связанный с выполнением функциональных обязанностей

Таблица 11

Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности организации:
Да
Нет
Нет, если это государственная организация
Да, если это государственная организация

Таблица 12

Пароль пользователя должен:
Содержать цифры и буквы разного регистра, знаки препинания, быть сложным для угадывания
Содержать только цифры
Содержать только буквы
Иметь привязку к пользователю

Таблица 13

Хищение информации - это:
Несанкционированное копирование информации
Утрата информации
Продажа информации

Приобретение информации

Таблица 14

Владельцем информации составляющей государственную тайну является:
Государство
Правительство Российской Федерации
Граждане
Президент

Таблица 15

Электронные замки "Соболь" предназначены для:
Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
Сканирования системы
Регистрации входа пользователей
Идентификации пользователей

Таблица 16

Информация об уголовной ответственности за преступления в сфере компьютерной информации описана:
28 главе Уголовного Кодекса
1 главе Уголовного Кодекса
в собрании уголовного законодательства Российской Федерации
в Уголовном Кодексе данный вопрос не регламентирован

7.3.3. Примерный перечень вопросов к зачетам и экзаменам

Зачет

Не предусмотрен учебным планом

Экзамен

1. Национальные интересы Российской Федерации в области информационной безопасности.
2. Основные угрозы безопасности. Информационная безопасность. Определение. Аспекты информационной безопасности. Направления обеспечения ИБ
3. Жизненно важные интересы и угрозы в информационной сфере. Уровни угроз ИБ и их классификация.
4. Отечественные и зарубежные стандарты в области информационной безопасности.
5. Защита информации. Определение. Формы и способы защиты. Политика безопасности и гарантированности.
6. Основные предметные направления защиты информации. Правовые основы защиты информации. Структура законодательства России в области защиты информации.
7. Источники права на доступ к информации. Информация как объект собственности: право владения, право пользования и право распоряжения. Федеральный Закон «Об информации, информатизации и защите информации».
8. Уровни доступа к информации с точки зрения законодательства. Виды досту-

па и механизмы доступа к информации.

9. Ответственность за нарушение законодательства в информационной сфере. Формы защиты права на доступ к информации.
10. Предмет и объекты защиты информации в автоматизированных системах обработки информации (АСОД). Надежность информации. Уязвимость информации.
11. Элементы и объекты защиты в АСОД. Основные элементы АСОД и типовые структурные компоненты.
12. Дестабилизирующие факторы АСОД. Причины нарушения целостности информации. Каналы несанкционированного получения информации в АСОД.
13. Преднамеренные угрозы безопасности АСОД. Атаки. Классификация угроз безопасности.
14. Функции и задачи защиты информации в АСОД. Механизм защиты.
15. Методы и системы защиты информации в АСОД. Целостность и конфиденциальность информации.
16. Аутентификация и идентификация. Подтверждение подлинности пользователей и разграничение их доступа к компьютерным ресурсам. Контроль доступа к аппаратуре.
17. Процедура опознавания с использование простого пароля. Методы проверки подлинности на основе динамически изменяющегося пароля.
18. Методы идентификации и установления подлинности субъектов и различных объектов. Функциональные методы.
19. Контроль информационной целостности. Организация контроля. Способы модификаций информации.
20. Защита информации от утечки по техническим каналам. Определения, понятия и виды каналов утечки.
21. Защита информации от утечки по визуально-оптическим и акустическим каналам.
22. Защита информации от утечки по электромагнитным и материально-вещественным каналам.
23. Технические средства защиты. Классификация технических средств. Функции защиты и степень сложности устройства.
24. Механические системы защиты. Системы оповещения. Системы опознавания. Оборонительные системы. Охранное освещение.
25. Физические средства защиты. Средства контроля доступа. Автоматизированные системы контроля доступа.
26. Биометрические системы идентификации. Основные методы. Охранные системы.
27. Криптографические методы защиты информации. Понятия и определения.
28. Криптология. Основные этапы ее развития.
29. Методы криптографического преобразования данных. Основные понятия и определения. Требования к криптографическим системам защиты.

30. Методы криптографического преобразования данных. Классификация. Виды криптографического закрытия.
31. Криптографическое закрытие данных шифрованием. Метода замены (подстановка). Полиалфавитная замена. Метод перестановки.
32. Криптографическое закрытие данных шифрованием. Метод гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы.
33. Криптографическое закрытие данных кодированием. Методы рассечение-разнесение и сжатия данных.
34. Криптосистемы. Понятие. Виды криптосистем. Стойкость криптосистем и их характеристики.
35. Криптосистемы с открытым ключом. Типы преобразований. Реализация процедуры шифрования с открытым ключом.
36. Электронная цифровая подпись (ЭЦП). Методы цифровой подписи, передаваемых в сети.
37. Криптографические стандарты DES и ГОСТ 28147-89.
38. Проблемы реализации методов криптографической защиты в АСОД.
39. Характеристики криптографических средств защиты.
40. Защита информации в персональных компьютерах. Особенности защиты.
41. Угрозы информации в персональных компьютерах. Классификация угроз. Виды каналов утечки.
42. Обеспечение целостности информации в персональных компьютерах (ПК). Защита ПК от несанкционированного доступа.
43. Физическая защита ПК и носителей информации. Опознавание (аутентификация) пользователей и используемых компонентов обработки информации.
44. Разграничение доступа к элементам защищаемой информации. Виды и характеристика способов доступа.
45. Регистрация обращений к защищаемой информации. Подсистема управления доступом. Подсистема регистрации и учета. Криптографическая система.
46. Защита информации от копирования. Основные функции систем защиты программ от копирования.
47. Защита от несанкционированного доступа к персональным компьютерам. Защита в средах Windows.
48. Защита ПК от вредоносных закладок. Классификация закладок и их общие характеристики.
49. Средства борьбы с вирусами и вредоносными закладками: юридические, организационно-административные, аппаратные и программные. Основные функции и мероприятия по защите.
50. Компьютерные вирусы. Классификация. Виды и характеристики.
51. Способы заражения программ компьютерными вирусами. Схема функционирования загрузочного вируса.
52. Признаки проявления компьютерных вирусов. Типы вирусных атак. Методы

профилактики и защиты.

53. Антивирусные программы. Виды и характеристики. Антивирусы-полифаги.
54. Антивирусные программы. Программы-ревизоры. Стадии работы: контроль оперативной памяти, контроль системных областей, контроль неизменяемых файлов.
55. Цели, функции и задачи защиты информации в сетях ЭВМ. Виды угроз.
56. Особенности защиты информации в вычислительных сетях. Понятие сервисов безопасности (механизмы защиты).
57. Безопасность и защита в базах данных. Механизмы управления доступом, удостоверения целостности данных, аутентификации, заполнения трафика, управления маршрутизацией и нотариального заверения.
58. Методы цифровой подписи данных, передаваемых в сети. Сущность метода распределения ключей при использовании: традиционных систем шифрования, систем шифрования с открытым ключом и методов цифровой подписи данных.
59. Системы защиты локальной вычислительной сети. Назначение системы защиты. Функциональное назначение подсистем: идентификации и аутентификации, разграничения доступа, управления доступом, контроля целостности, регистрации событий безопасности.
60. Межсетевые экраны-брандмауэры (FireWall). Назначение и функциональные возможности.

Примерный перечень практических заданий на экзамен

1. Проанализировать разделы, структуру в целом, физического диска персонального компьютера.

2. Произвести разграничение доступа к локальным и сетевым ресурсам, провести аудит системы безопасности стандартными средствами операционной системы семейства Windows.

3. Использование возможностей защиты документа, а также ЭЦП при работе с текстовым редактором Microsoft Word.

4. Использование возможностей защиты документа, а также ЭЦП при работе с табличным редактором Microsoft Excel.

5. Создание архивов данных с использованием парольной защиты, исследование парольной защиты программных архиваторов RAR, ZIP, ARJ.

6. Восстановление информации на носителей информации.

7. Обнаружение и удаление компьютерных вирусов средствами антивирусной защиты информации.

8. Анализ угроз информационной безопасности на объектах информатизации использующих информационные системы обработки персональных данных.

9. Обзор методов криптографии. Шифрование и дешифрование данных криптографическими методами преобразования.

7.3.4 Примерный перечень тем докладов (рефератов) дисциплины выносимых на самостоятельную работу

Реферат является одной из форм отчётности по итогам курса, он позволяет структурировать знания обучаемых. Реферат письменный доклад или выступление по определённой теме с обобщением информации из одного или нескольких источников.

Реферат предполагает осмысленное изложение содержания главного и наиболее важного (с точки зрения автора) в научной литературе по определенной проблеме в письменной или устной форме.

Этапы работы над рефератом

Выбор темы. Очень важно правильно выбрать тему. Выбор темы не должен носить формальный характер, а иметь практическое и теоретическое обоснование. Автор реферата должен осознанно выбрать тему с учетом его познавательных интересов. Если интересующая тема отсутствует в рекомендательном списке, то по согласованию с преподавателем студенту предоставляется право самостоятельно предложить тему реферата, раскрывающую содержание изучаемой дисциплины. Тема не должна быть слишком общей и глобальной, так как небольшой объем работы (до 20 страниц) не позволит раскрыть ее.

После выбора темы составляется список изданной по теме (проблеме) литературы, опубликованных статей, необходимых справочных источников.

Составление плана. Автор по предварительному согласованию с преподавателем может самостоятельно составить план реферата, с учетом замысла работы, либо взять за основу рекомендуемый план.

Наиболее традиционной является следующая структура реферата:

Титульный лист.

Оглавление (план, содержание).

Введение.

Глава 1 (полное наименование главы).

1.1. (полное название параграфа, пункта);

1.2. (полное название параграфа, пункта).

Глава 2 (полное наименование главы). Основная часть

2.1. (полное название параграфа, пункта);

2.2. (полное название параграфа, пункта).

Заключение (или выводы).

Список использованной литературы.

Приложения (по усмотрению автора).

Оглавление (план, содержание) включает названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в текст реферата.

Введение. В этой части реферата обосновывается актуальность выбранной темы, формулируются цели работы и основные вопросы, которые предполагается раскрыть в реферате, указываются используемые материалы и дается их

краткая характеристика с точки зрения полноты освещения избранной темы. Объем введения не должен превышать 1-1,5 страницы.

Основная часть реферата может быть представлена одной или несколькими главами, которые могут включать 2-3 параграфа (подпункта, раздела). Здесь достаточно полно и логично излагаются главные положения в используемых источниках, раскрываются все пункты плана с сохранением связи между ними и последовательности перехода от одного к другому. Автор должен следить за тем, чтобы изложение материала точно соответствовало цели и названию главы (параграфа). Материал в реферате рекомендуется излагать своими словами, не допуская дословного переписывания из литературных источников. В тексте обязательны ссылки на первоисточники, т.е. на тех авторов, у которых взят данный материал в виде мысли, идеи, вывода, числовых данных, таблиц, графиков, иллюстраций и пр.

Работа должна быть написана грамотным литературным языком.

Сокращение слов в тексте не допускается, кроме общеизвестных сокращений и аббревиатуры. Каждый раздел рекомендуется заканчивать кратким выводом.

Заключение (выводы). В этой части обобщается изложенный в основной части материал, формулируются общие выводы, указывается, что нового лично для себя вынес автор реферата из работы над ним. Выводы делаются с учетом опубликованных в литературе различных точек зрения по проблеме рассматриваемой в реферате, сопоставления их и личного мнения автора реферата.

Заключение по объему не должно превышать 1,5-2 страниц.

Приложения могут включать графики, таблицы, расчеты. Они должны иметь внутреннюю (собственную) нумерацию страниц.

Библиография (список литературы) здесь указывается реально использованная для написания реферата литература, периодические издания и электронные источники информации. Список составляется согласно правилам библиографического описания.

Приблизительные темы:

1. Социальный инжиниринг как угроза информационной безопасности.
2. Организация антивирусной защиты на типовом объекте информатизации.
3. Использование криптографических систем защиты информации
4. Компьютерная преступность и компьютерная безопасность
5. Виды ответственности за нарушения в сфере информационного права
6. Использование комплексных решений при защите информации от утечек по техническим каналам.
7. Защита информации при работе с почтовыми сообщениями
8. Вопросы организации защиты информации при работе с базами данных.
9. Защита информации от несанкционированного доступа с использованием криптографических методов.
10. Обеспечение информационной безопасности при работе в сети Интернет.
11. Источники возникновения угроз информационной безопасности.

12. Анализ сетевого трафика как инструмент информационной безопасности.
13. Обеспечение информационной безопасности в локальной вычислительной сети.
14. Персональные данные как объект защиты информации.
15. Каналы утечки информации
16. Защита информации в информационных системах персональных данных.
17. Побочные электромагнитные излучения и наводки как угроза информационной безопасности.
18. Криптографические методы защиты информации.
19. Вредоносное программное обеспечение как угроза целостности информации.
20. Использование антивирусного программного обеспечения.
21. Организационные методы защиты информации.
22. Использование модели угроз информационной безопасности в современных условиях.
23. Компьютерные вирусы как угроза информационной безопасности.
24. Нормативные правовые основы информационной безопасности в Российской Федерации.
25. Обзор современных стандартов информационной безопасности.
26. Классификация угроз информационной безопасности.
27. Классификация компьютерных вирусов и антивирусного программного обеспечения.
28. Межсетевые экраны как средство защиты информации в информационной системе.
29. Принципы обеспечения защиты информации в распределенных информационных системах.
30. Классификация удаленных угроз информационной безопасности в распределенных информационных системах и их характеристика.

7.3.5. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции или ее части	Наименование оценочного средства
1.	Основные аспекты профессиональной подготовки будущих специалистов в сфере информационных систем и технологий	ОПК-4	Реферат (Р) Экзамен (Э) Защита курсового проекта (КП)
2.	Методологические основы информационной безопасности	ОПК-4, ПК-1, ПК-6, ДПК-4	Реферат (Р) Защита лабораторных работ (ЗЛР) Экзамен (Э) Тестирование (Т)
3.	Базовые принципы информационной безопасности, их характеристика и модели	ОПК-4, ПК-1, ПК-6, ДПК-4	Реферат (Р) Защита лабораторных работ (ЗЛР) Экзамен (Э) Защита курсового проекта

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции или ее части	Наименование оценочного средства
			(КП) Тестирование (Т)
4.	Обзор и характеристика базовых информационных технологий.	ОПК-4, ПК-1, ПК-6, ДПК-4	Реферат (Р) Защита лабораторных работ (ЗЛР) Защита практических работ (ЗПР) Экзамен (Э) Защита курсового проекта (КП) Тестирование (Т)
5.	Обзор и характеристика прикладных информационных технологий	ОПК-4, ПК-1, ПК-6, ДПК-4	Реферат (Р) Защита лабораторных работ (ЗЛР) Экзамен (Э) Защита курсового проекта (КП) Тестирование (Т)
6.	Характеристика инструментальной базы информационных технологий в сфере информационной безопасности	ОПК-4, ПК-1, ПК-6, ДПК-4	Реферат (Р) Защита лабораторных работ (ЗЛР) Экзамен (Э) Тестирование (Т)

7.4. Порядок процедуры оценивания знаний, умений, навыков и (или) опыта деятельности на этапе промежуточного контроля знаний

При проведении устного экзамена обучающемуся предоставляется 60 минут на подготовку. Опрос обучающегося по билету на устном экзамене не превышает двух астрономических часов. С экзамена снимается материал тех самостоятельных работ и курсовых работ, которые обучающийся выполнил в течение семестра на «хорошо» и «отлично». Во время проведения экзамена (зачета) обучающиеся могут пользоваться программой дисциплины, а также вычислительной техникой.

8. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	Наименование издания	Вид издания (учебник, учебное пособие, методические указания, компьютерная программа)	Автор (авторы)	Год издания	Место хранения и количество

9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторном или практическом занятии
Лабораторные занятия	Работа студентов на лабораторных занятиях нацелена на практическом закреплении теоретических вопросов в области обеспечения информационной безопасности. В рамках, которых студенты выполняют задания по созданию исчерпывающего списка потенциальных угроз информационной безопасности на объекте информатизации, определение количественных показателей и выбором приемлемых средств защиты информации. Работают над построением архитектуры системы защиты информации объекта информатизации и обоснованием применяемых мерах по защите информации. С целью практического закрепления вопросов организации идентификации (аутентификации), разграничения доступа пользователей к ресурсам информационных систем выполнение заданий осуществляется с использованием средств виртуализации, задействованных при построении локальных сетей под управлением как пользовательских так и серверных операционных систем семейства Windows. Так же у студентов закрепляется навык работы с сертифицированным антивирусным программным обеспечением, как инструментом, обеспечивающим защиту информации от воздействия вредоносного программного обеспечения.
Курсовая работа	В процессе работы над курсовым проектом студент более глубоко знакомится с основными источниками знаний в области информационной безопасности и защиты информации, включая международное право, стандарты (международные, отраслевые, национальные и т.д.). В процессе работы над курсовым проектом студенту необходимо провести объективный анализ предметной области с учетом заданной тематики. С учетом проведенного анализа определяется роль и место "изучаемой проблемы" в вопросе обеспечения защиты информации и информационной безопасности на объектах информатизации. Студентом даются конкретные предложения по использованию средств защиты информации, с учетом модели угроз информационной безопасности.
Подготовка к экзамену (зачету)	При подготовке к экзамену (зачету) необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и выполнение заданий на лабораторных и практических занятиях.

10.УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

10.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля):

10.1.1Основная литература:

1. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов : допущено УМО / под ред. С. А. Клейменова. - Москва : Academia, 2006 (Саратов : Саратовский полиграф. комбинат, 2006). - 330 с

2. Девянин П. Н. Модели безопасности компьютерных систем : Девянин, П. Н. - М. Academia, 2005 - 142 с.

3. Белов, Е. Б. Основы информационной безопасности / - М. : Горячая линия-Телеком, 2006. – 544 с./Основы информационной безопасности : Учебное пособие / Белов Е. Б. - Москва : Горячая линия - Телеком, 2011. - 558 с. - ISBN 5-93517-292-5. URL: http://www.iprbookshop.ru/12014

10.1.2 Дополнительная литература:

1. Скрипник, Д. А. Обеспечение безопасности персональных данных : учебное пособие / Скрипник Д. А. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2011. - 91 с. URL: http://www.iprbookshop.ru/16708

2. Фороузан, Бехроуз. Криптография и безопасность сетей : Учебное пособие / ФороузанБехроуз. - Москва : БИНОМ. Лаборатория знаний, Интернет-Университет Информационных Технологий (ИНТУИТ), 2010. - 784 с. - ISBN 978-5-9963-0242-0. URL: http://www.iprbookshop.ru/15847

3. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]/ Авдошин С.М., Савельева А.А., Сердюк В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2010.— 326 с.— Режим доступа: http://www.iprbookshop.ru/16737

4. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2012.— 159 с.— Режим доступа: http://www.iprbookshop.ru/15425

10.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем:

- . Персональные компьютеры с операционной системой Windows 7*.
- Microsoft Office

– Internet
– Total Commander
– MS Visio2007
– MS Access 2007
– Visual Basic
– Браузеры: Chrome, Firefox, Opera, Safari, IE;
– http://www.edu.ru/modules.php
– http://www.structuralist.narod.ru
– http://www.info-system.ru/tech_doc/tech_doc.html
– http://www.it-konsultant.ru
– http://www.gostbaza.ru/
– www.consultant.ru

10.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля):

– http://www.citforum.ru/
– http://www.itshop.ru
– http://valera.asf.ru/cpp/scpp/
– http://saod.net/saod2/index.html

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

При освоении дисциплины для проведения лекционных занятий нужны учебные аудитории, оснащённые мультимедийным оборудованием, для выполнения лабораторных работ необходимы классы персональных компьютеров с набором базового программного обеспечения.

12. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (образовательные технологии)

При реализации программы дисциплины «Информационная безопасность и защита информации» используются различные образовательные технологии с учетом внедрения инновационных приемов и способов обучения при одновременном использовании традиционных методик.

Лекционный курс содержит теоретический и практический материал, отражающий современное состояние научных концепций по данной тематике и снабженный примерами. В процессе лекционного занятия студенты слушают преподавателя, задают вопросы, часть информации конспектируют. Лекционные занятия дополняются демонстрацией слайдов с использованием ПК и проектора, концентрирующих внимание слушателей на ключевых моментах лекци-

онного материала.

Лабораторные работы занятия проводятся в форме:

а) занятия, предполагающего:

- владение компьютерными технологиями студентов на основе результатов входного контроля по тестовым заданиям по работе с типовым программным обеспечением. Далее по темам дисциплины каждый студент получает индивидуальное задание, выполнение которого подразумевает использование современных компьютерных технологий, и участвует в решении поставленной задачи. В течение семестра студенты выполняют задачи, указанные преподавателем к каждому занятию.

б) контрольного занятия.

Проведение лекционных, практических и лабораторных занятий осуществляется с постановкой проблемных вопросов, допускающих возникновение дискуссий, решение совместных практических задач, что предполагает активное включение студентов в образовательный процесс.

На самостоятельную работу выносятся следующие виды деятельности:

- проработка лекций и подготовка к лабораторным и практическим работам - включает чтение конспекта лекций, профессиональной литературы, периодических изданий;

- решение и подготовка индивидуальных задач на лабораторное занятие – проводится под контролем преподавателя;

- подготовка реферата (контрольная работа для заочной формы обучения);

По завершении тем, для закрепления материала рекомендуется выдача самостоятельных заданий в виде реализации практических заданий по изученным темам.

Рекомендуется практиковать написание и заслушивание кратких докладов студентов по изучаемым темам.

При изучении дисциплины целесообразно использовать материалы интернет–ресурсов образовательной, аналитической направленности.

Традиционная лекция имеет несколько ограниченные возможности формирования в сознании студентов ярких представлений элементов изучаемого материала, несущих смысловую нагрузку. Поэтому компьютерная демонстрация лекционного материала является одним из решений изложенной выше проблемы. Лекция должна побуждать к познанию и творческому поиску, а также служить примером использования современных технологий. При представлении электронных презентаций подача информации преподносится модулями на «зрительном», «графическом» и «звуковом» уровнях, что является важным фактором для улучшения восприятия лекционного материала студентами.

Для сопровождения всего лекционного занятия или отдельной его части: этапа мотивации, изучения нового материала, контроля за усвоением используются слайды, созданные с помощью программы графических презентаций Power Point. Состав информационных объектов определяется особенностями конкретной темы и целевым назначением занятия. В качестве демонстрируемых фрагментов могут быть использованы текстовые материалы, статические и динамические изображения, контрольные задания и т. п. Для эффективного предъявления учебного материала применяются мультимедийные средства отображения информации.

На визуализированной лекции удобно осуществлять обратную связь. Для этого можно на завершающем этапе лекции предложить студентам выбрать правильные из имеющихся вариантов ответов на несколько простых вопросов по всему изученному на занятии материалу. Форма контроля определяется уровнем подготовленности студентов, содержанием учебного материала.

Таким образом, используя современные программно-технические средства, преподаватель имеет возможность проводить более наглядные и информационно насыщенные занятия, иллюстрировать каждое новое понятие и его связи с соответствующими задачами практики; и тем самым улучшить процесс восприятия и усвоения материала.

Система контрольных мероприятий должна обеспечивать объективную оценку знаний и навыков студентов, способствовать повышению эффективности всех видов учебных занятий, включая и самостоятельную работу.

Для освоения всех разделов дисциплины эффективно использование обучающих и контролирующих компьютерных программ. При освоении всех разделов дисциплины необходимо сочетание различных форм учебной деятельности: изучение лекционного материала, выполнение заданий на практических занятиях, как с использованием компьютера, так и без него, самостоятельная работа с рекомендуемой литературой и использование методических указаний, консультации преподавателей при выполнении дополнительных заданий.

При реализации различных видов учебной работы используются следующие образовательные технологии:

1. Лекционные занятия проводятся с широким использованием активных и интерактивных форм, в том числе мультимедийных технологий (презентации).

2. На лабораторных занятиях используются интерактивные формы проведения занятий.

3. Внеаудиторная работа широко использует возможности Интернет и другие информационные источники, с целью самостоятельного формирования и развития профессиональных навыков обучающихся.

По завершении тем, для закрепления материала рекомендуется выдача самостоятельных заданий по изученным темам. Рекомендуется практиковать написание и заслушивание кратких докладов студентов по изучаемым темам.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 «Информационные системы и технологии».

Руководитель основной образовательной программы

канд. техн. наук, доцент
кафедры информационных технологий
и автоматизированного
проектирования в
строительстве _____/О.В. Курипта /

Рабочая программа одобрена учебно-методической комиссией факультета «Экономики, менеджмента и информационных технологий»

«07» сентября 2017г., протокол № 3

Председатель доктор техн. наук, профессор _____ Курочка П.Н.
учёная степень и звание, подпись инициалы, фамилия

Эксперт

ВГУИТ к.т.н. доцент _____ С.Г. Мартынов
(место работы) (занимаемая должность) (подпись) (инициалы, фамилия)

М П
организации

федеральное государственное бюджетное образовательное учреждение высшего образования
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»
Подпись т. Мартынова С.Г.
07.09.2017 ЗАВЕРЯЮ
Начальник управления кадров Н.А. Кочева