МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)

Кафедра _____Информационный и электронный сервис_____

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

по дисциплине _____«Защита информации»_____

для студентов специальностиподготовки __09.02.01 «Компьютерные системы и комплексы»___

Тольятти 2018

2

Рабочая учебная программа по дисциплине "Защита информации" разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 09.02.01 «Компьютерные системы и комплексы»
решением Президиума Ученого совета

Протокол № 4 от 28.06.2018 г.

Начальник учебно-методического отдела_____ Н.М.Шемендюк

28.06.2018 г.

3

Рабочая учебная программа по дисциплине «Защита информации» разработана в соответствии с Федеральными государственными образовательными стандартами: специальности 09.02.01 «Компьютерные системы и комплексы» утвержденный приказом Министерства образования и науки Российской Федерации от 28.07.2014 №849.

Составил: к.т.н., доцент Жуков Г.П

СОГЛАСОВАНО:
Директор научной библиотеки _____ В.Н.Еремина

СОГЛАСОВАНО:
Начальник управления информатизации _____ В.В.Обухов

Рабочая программа утверждена на заседании кафедры «Информационный и электронный сервис»

Протокол № 11 от «27» июня 2018 г.

Заведующий кафедрой _____ д.т.н., профессор В.И. Воловач
(подпись)

СОГЛАСОВАНО:
Начальник учебно-методического отдела _____ Н.М.Шемендюк

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Цели освоения дисциплины

Целями освоения дисциплиныявляются: изучение основных понятий и определений защиты информации; источников риска и форм атак на компьютерную информацию; политики безопасности и законодательно – правовые и организационные методы защиты компьютерной информации; изучение методов и средств защиты компьютерной информации.

1.2. В соответствии с видами профессиональной деятельности, на которые ориентирована образовательная программа указанногонаправления подготовки,содержание дисциплиныпозволит обучающимся решать следующие профессиональные задачи:
политики безопасности и законодательно – правовые и организационные методы защиты компьютернойинформации; защиты информации в компьютерных системах и комплексах.

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплиныу обучающихся формируются следующие компетенции:

Кодкомпетенции	Наименованиекомпетенции
ПК-1.4	Проводить измерения параметров проектируемых устройств и определять показатели надежности
ПК-2.2	Производить тестирование, определение параметров и отладку микропроцессорных систем
ПК-3.1	Проводить контроль параметров, диагностику и восстановление работоспособности компьютерных систем и комплексов.

1.4.Перечень планируемых результатов обучения по дисциплине

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
Знает: (ПК-1.4, ПК-2.2, ПК-3.1) мероприятия по защите информации в компьютерных системах и комплексах. Основные понятия и определения защиты информации в компьютерных системах, комплексах и сетях; источники риска и форм атак на компьютерную информацию; политику и стандарты безопасности; аппаратные и программные	*Лекции*	*Собеседование, опрос, оценка*

средства контроля и диагностики компьютерных систем и комплексов; методы и средства обеспечения информационной безопасности компьютерных систем		
Умеет: (ПК-1.4, ПК-2.2, ПК-3.1) решать задачи по защите информации в компьютерных системах и комплексах; проводить контроль, диагностику и восстановление работоспособности компьютерных систем и комплексов; выявлять угрозы информационной безопасности	*Лабораторные работы*	*Защита лабораторных работ, оценка*
Имеет практический опыт: (ПК-1.4, ПК-2.2, ПК-3.1) использования мероприятий по защите информации в компьютерных системах и комплексах.	*Лабораторные работы*	*Защита лабораторных работ, оценка*

2. Место дисциплиныв структуре образовательной программы

Дисциплинаотносится к _____вариативной_____части.
(базовой, вариативной)

Ее освоение осуществляется в _____5__(7_з/о)____семестре(ах).*

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код компетенции(й)
	Предшествующие дисциплины(практики)	
1	Информатика и ИКТ	ОК-1 – ОК 9
	Последующие дисциплины(практики)	
3	Операционные системы и среды	ОК-1 – ОК 9; ПК 2.3; ПК 3.3; ПК 4.3

*Здесь и далее семестры указаны для обучающихся на базе основного общего образования. Для лиц, обучающихся на базе среднего общего образования, семестры соответствуют учебному плану и нормативному сроку обучения, установленному ФГОС.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Распределение фонда времени по семестрами видам занятий

Виды занятий	очная форма обучения		заочная форма обучения
Итого часов	58 ч.		58 ч.
Лекции (час)	20		4
Практические (семинарские) занятия (час)	-		-
Лабораторные работы(час)	28		2
Самостоятельная работа (час)	10		52
Курсовой проект (работа) (+,-)	-		-
Контрольная работа (+,-)	-		-
Экзамен, семестр /час.			
Зачет (дифференцированный зачет), семестр	6		6/4
Контрольная работа, семестр	-		-

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины	Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в академических часах)				Средства и технологии оценки
		Лекции, час	кие (семинарские) занятия.	Лабораторные работы, час	Самостоятельная работа, час	
1	Основные понятия и определения защиты информации. Источники риска и формы атак на компьютерную информацию. Компьютерныеатаки и технологииихобнаружения	4/-/1	-/-/-	-/-/-	2/-/10	Конспект
2	Политика и стандарты безопасности. Законодательно – правовые и организационные методы защиты компьютерной информации.	2/-/1	-/-/-	4/-/-	2/-/8	Конспект, защита лабораторных работ
3	Криптографические модели и методы защиты информации. Алгоритмышифрования	4/-/1	-/-/-	8/-/2	1/-/8	Конспект, защиталабораторныхработ
4	Методы и средства защиты информации от несанкционированного доступа.	4/-/-	-/-/-	16/-/2	1/-/8	Конспект, защита лабораторных работ

	Алгоритмыаутентификациипользователей					
5	Модели безопасности основных ОС. Администрирование сетей.	2/-/-	-/-/-	-/-/-	2/-/8	Конспект, защита лабораторных работ
6	Требования к системам защиты информации. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Построениекомплексныхсистем защитыинформации.	4/-/1	-/-/-	-/-/2	2/-/10	Конспект, защита лабораторных работ
	Аттестация по дисциплине	20/-/4	-/-/-	28/-/2	10/-/52	Зачет

Примечание:
-/-/-, объем часов соответственно для очной, очно-заочной, заочной форм обучения

4.2.Содержание практических (семинарских) занятий

Практические работы учебным планом не предусмотрены

4.3.Содержание лабораторных работ(при наличии в учебном плане)

№	Наименование лабораторных работ	Обьем часов	Наименование темы дисциплины
	__5 (7 з/о)__ **семестр**		
1	Лабораторная работа1. Российское законодательство по защите компьютерной информации. Компьютерные преступления	4/-/-	Тема 2. Политика и стандарты безопасности. Законодательно – правовые и организационные методы защиты компьютерной информации.
2	Лабораторная работа 2. Криптографические методы защиты информации. Алгоритмы шифрования	8/-/2	Тема 3. Криптографические модели и методы защиты информации. Алгоритмы шифрования
3	Лабораторная работа 3. Основные признаки присутствия на компьютере вредоносных программ	2/-/-	Тема 5. Модели безопасности основных ОС. Администрирование сетей.
4	Лабораторная работа 4. Установка и предварительная настройка Антивируса Касперского	4/-/-	Тема 5. Модели безопасности основных ОС. Администрирование сетей.
5	Лабораторная работа 5. Начало работы с Антивирусом Касперского	4/-/-	Тема 5. Модели безопасности основных ОС. Администрирование сетей
6	Лабораторная работа 6. Диагностика Антивируса Касперского	4/-/-	Тема 5. Модели безопасности основных ОС. Администрирование сетей
7	Лабораторная работа 7. Обновление антивирусных баз	2/-/-	Тема 5. Модели безопасности основных ОС. Администрирование сетей
	Итого за ___5 (7 з/о)_ семестр	28/-/2	
	Итого	28/-/2	

5. Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине

Технологическая карта самостоятельной работы студента

Код реализуемой компетенции	Вид деятельности студентов (задания на самостоятельную работу)	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов
ПК-1.4, ПК-2.2, ПК-3.1	Основные понятия и определения защиты информации. Источники риска и формы атак на компьютерную информацию. Компьютерныеатаки и технологииихобнаружения	Конспект	Собеседование	2/-/10
ПК-1.4, ПК-2.2, ПК-3.1	Политика и стандарты безопасности. Законодательно – правовые и организационные методы защиты компьютерной информации.	Конспект, защита лабораторных работ	Собеседование	2/-/8
ПК-1.4, ПК-2.2, ПК-3.1	Криптографические модели и методы защиты информации. Алгоритмы шифрования	Конспект, защиталабораторных работ	Собеседование	1/-/8
ПК-1.4, ПК-2.2, ПК-3.1	Методы и средства защиты информации от несанкционированного доступа. Алгоритмы аутентификации пользователей	Конспект, защита лабораторных работ	Собеседование	1/-/8
ПК-1.4, ПК-2.2, ПК-3.1	Модели безопасности основных ОС. Администрирование сетей.	Конспект, защита лабораторных работ	Собеседование	2/-/8
ПК-1.4, ПК-2.2, ПК-3.1	Требования к системам защиты информации. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Построениекомплексныхсистемзащитыинформации.	Конспект, защита лабораторных работ	Собеседование	2/-/10
			Итого за _5 (7 з/о)__семестр	10/-/52
			Итого	10/-/52

Рекомендуемая литература

1. Васильков, А. В. Безопасность и управление доступом в информационных системах[Электронный ресурс] : учеб. пособие для сред. проф. образования / А. В. Васильков, И. А. Васильков. - Документ Bookread2. - М. : ФОРУМ [и др.], 2017. - 367 с. : ил., табл. - Режим доступа: http://znanium.com/bookread2.php?book=537054.
2. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты информации[Электронный ресурс] : учеб. для сред. проф. образования по специальности 10.02.01 "Орг. и технология защиты информации" / В. П. Зверева, А. В. Назаров. -

Документ Bookread2. - М. : Курс [и др.], 2017. - 317 с. - Режим доступа: http://znanium.com/bookread2.php?book=635130.

3. Эксплуатация объектов сетевой инфраструктуры[Текст] : учеб. для сред. спец. образования по специальности "Компьютер. сети" / А. В. Назаров [и др.] ; под ред. А. В. Назарова. - М. : Академия, 2014. - 368 с. : ил.

Содержание заданий для самостоятельной работы

Темы рефератов

1.Законы РФ о защите информации
2.Основные положения УК «О компьютерных преступлениях»
3.Антивирусные программные средства

Письменные работы могут быть представлены в различных формах:

- реферат - письменныйдоклад иливыступлениепоопределённойтеме, вкоторомсобранаинформацияизодногоилинесколькихисточников.

Рефератымогутявлятьсяизложениемсодержаниянаучнойработы, художественнойкнигии т. п.

- другое.

Вопросы (тест) для самоконтроля

1.Угрозы безопасности информационным системам классифицируют
2.Кто осуществляет общее руководство системой информационной безопасности в РФ
3.Назовите Законы РФ о защите информации
…

Индивидуальные (групповые) задания для самостоятельной работы

1.Выполнить проверку носителя информации с помощью Антивируса Касперского
2.Выполнить Обновление антивирусных баз программы Касперского.

…

6. Методические указания для обучающихся по освоению дисциплины

Инновационные образовательные технологии

Вид образовательных технологий, средств передачи знаний, формирования умений и практического опыта	№ темы / темалекции	№ практического (семинарского) занятия/наименование темы	№ лабораторной работы / цель
Слайд-лекции	1/ Основные понятия и определения защиты информации. Источники риска и формы атак на компьютерную информацию. Компьютерные атаки и технологии их обнаружения. 2/ Политика и стандарты безопасности. Законодательно – правовые и организационные методы защиты компьютерной информации.	-	1/ закрепить теоретические знания полученные на лекционных занятиях. 2/ закрепить теоретические знания полученные на

	3/ Криптографические модели и методы защиты информации. Алгоритмы шифрования. 4/ Методы и средства защиты информации от несанкционированного доступа. Алгоритмы аутентификации пользователей. 5/ Модели безопасности основных ОС.Администрирование сетей. 6/ Требования к системам защиты информации. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Построениекомплексныхсистемзащитыинформации.		лекционных занятиях. 3/ освоить основы криптографические модели и методы защиты информации 4/освоить основные признаки присутствия на компьютере вредоносных программ 5,6,7/освоить установку и настройку Антивируса Касперского;начало работы и диагностику Антивируса Касперского;обновлять антивирусную базу

В начале семестра студентам необходимо ознакомиться с технологической картой дисциплины, выяснить, какие результаты освоения дисциплины заявлены (знания, умения, практический опыт). Для успешного освоения дисциплиныстудентам необходимо выполнить задания, предусмотренные рабочей учебной программой дисциплиныи пройти контрольные точки в сроки, указанные в технологической карте (раздел 11).От качества и полноты их выполнения будет зависеть уровень сформированности компетенции и оценка текущей успеваемости по дисциплине. По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации, если это предусмотрено технологической картой дисциплины. Списки учебных пособий, научных трудов, которые студентам следует прочесть и законспектировать, темы практических занятий и вопросы к ним, вопросы к экзамену (зачету) и другие необходимые материалы указаны в разработанном для данной дисциплиныучебно-методическом комплексе.

Основной формой освоения дисциплины является контактная работа с преподавателем - лекции, практические занятия, лабораторные работы (при наличии в учебном плане), консультации (в том числе индивидуальные), в том числе проводимые с применением дистанционных технологий.

По дисциплине часть тем (разделов) изучается студентами самостоятельно. Самостоятельная работа предусматривает подготовку к аудиторным занятиям, выполнение заданий (письменных работ, творческих проектов и др.) подготовку к промежуточной аттестации (экзамену (зачету)).

На лекционных и практических (семинарских) занятиях вырабатываются навыки и умения обучающихся по применению полученных знаний в конкретных ситуациях, связанных сбудущей профессиональной деятельностью. По окончании изучения дисциплины проводится промежуточная аттестация (экзамен, (зачет)).

Регулярное посещение аудиторных занятий не только способствует успешному овладению знаниями, но и помогает организовать время, т.к. все виды учебных занятий распределены в семестре планомерно, с учетом необходимых временных затрат.

6.1.Методические указания для обучающихся по освоению дисциплинына практических (семинарских) занятиях, лабораторных работах *(указать нужное)*

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;

- получение навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;

- обсуждение вопросов в аудитории, разделенной на группы 6 - 8 обучающихся либо индивидуальных;

- выполнение практических заданий, задач;

- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины;

- другое.

Содержание заданий для практических занятий

Практические занятияпо дисциплинеучебным планом не предусмотрена

Лабораторныеработы

№	Наименование лабораторных работ	Задание по лабораторным работам
1	Российское законодательство по защите компьютерной информации. Компьютерные преступления	1.Основные понятия защиты компьютерной информации. 2.Компьютерные преступления и особенности их раскрытия. 3.Законодательство РФ в области информационной безопасности
2	Криптографические методы защиты информации. Алгоритмы шифрования	1. Криптографические методы защиты информации. 2. Алгоритмы шифрования
3	Основные признаки присутствия на компьютере вредоносных программ	Задание 1. Изучение настроек браузера Задание 2. Подозрительные процессы Задание 3. Элементы автозапуска Задание 4. Сетевая активность
4	Установка и предварительная настройка Антивируса Касперского	Подготовительная часть. Задание 1. Системные требования Задание 2. Установка Антивируса Касперского
5	Начало работы с Антивирусом Касперского	Задание 1. Изучение интерфейса Задание 2. Структура и настройки Задание 3. Постоянная защита Задание 4. Поиск вирусов Задание 5. Сервис

6	Диагностика Антивируса Касперского	Задание 1. Тестовый вирус Задание 2. Тестирование с помощью EICAR Задание 3. Лечение инфицированных файлов Задание 4. Помещение файлов на карантин
7	Обновление антивирусных баз	Задание 1. Настройка обновления Задание 2. Запуск процедуры обновления

Лабораторные работы обеспечивают:

формирование умений и навыков обращения с приборами и другим оборудованием, демонстрацию применения теоретических знаний на практике, закрепление и углубление теоретических знаний, контроль знаний и умений в формулировании выводов, развитие интереса к изучаемой дисциплине.

Применение лабораторных работ позволяет вовлечь в активную работу всех обучающихся группы и сформировать интерес к изучению дисциплины.

Самостоятельный поиск ответов на поставленные вопросы и задачи в ходе лабораторной работы приобретают особую значимость в восприятии, понимании содержания дисциплины.

Изученный на лекциях материал лучше усваивается, лабораторные работы демонстрируют практическое их применение.

6.2.Методические указания для выполнения контрольных работ(при наличии)

Контрольная работапо дисциплинеучебным планом не предусмотрена.

6.3. Методические указания для выполнения курсовых работ (проектов)

Курсовая работа (проект)по дисциплинеучебным планом не предусмотрена.

7. Паспортфонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (зачет)

Фонды оценочных средств, позволяющие оценить уровень сформированности компетенций и результаты освоения дисциплины, представлены следующими компонентами:

Код оцениваемой компетенции (или ее части)	Этап формирования компетенции *(№ темы)*	Тип контроля	Вид контроля	Количество элементов
ПК-1.4, ПК-2.2, ПК-3.1	*1-6*	*Промежуточный тест*	*устный опрос, компьютерный тест*	*1-17*

7.1.Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Результаты освоения дисциплины	**Оценочные средства**(перечень вопросов, заданий и др.)
*№ компет(*ПК-1.4, ПК-2.2, ПК-3.1) ***Знает:*** мероприятия по защите информации в компьютерных системах и комплексах. Основные понятия и определения защиты информации в компьютерных системах, комплексах и сетях; источники риска и форм атак на компьютерную информацию; политику и стандарты безопасности; аппаратные и программные средства контроля и диагностики компьютерных систем и комплексов; методы и средства обеспечения информационной безопасности компьютерных систем.	1.Кто в РФ осуществляет Общее руководство системой информационной безопасности осуществляют 2.В каком году был принятзакон РФ «Об информации, информационных технологиях и о защите информации» 3.Аутентификация субъекта — это 4.Как классифицируются угрозы безопасности информационным системам 5.Политика безопасности - это 6.Алгоритмы криптографического преобразования информации - это 7.Доступ к информации различают 8.Санкционированный доступ к информации — это 9.Несанкционированный доступ к информации характеризуется 10.Угрозы безопасности ИС по природе возникновения бывают
*№ компет(*ПК-1.4, ПК-2.2, ПК-3.1) ***Умеет:*** решать задачи по защите информации в компьютерных системах и комплексах; проводить контроль, диагностику и восстановление работоспособности компьютерных систем и комплексов; выявлять угрозы информационной безопасности	11.Определять признаки присутствия на компьютере вредоносных программ 12.Установить и предварительно настроить Антивируса Касперского 13.Начать работу с Антивирусом Касперского 14.Выполнять диагностику Антивируса Касперского 15.Выполнить обновление антивирусных баз
*№ компет(*ПК-1.4, ПК-2.2, ПК-3.1) ***Имеет практический опыт*** использования мероприятий по защите информации в компьютерных системах и комплексах	16.Выполнить проверку носителя информации с помощью Антивируса Касперского 17.Выполнить Обновление антивирусных баз программы Касперского

7.2. Методические рекомендации к определению процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Рабочая учебная программа дисциплинысодержит следующие структурные элементы:

-перечень компетенций, формируемых в результате изучения дисциплины с указанием этапов их формирования в процессе освоения образовательной программы;

-типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования

компетенций в процессе освоения образовательной программы (далее–задания). Задания по каждой компетенции, как правило, не должны повторяться.

Требования по формированию задания на оценку ЗНАНИЙ:

-обучающийся должен воспроизводить и объяснять учебный материал с требуемой степенью научной точности и полноты;

-применяются средства оценивания компетенций: тестирование, вопросы по основным понятиям дисциплиныи т.п.

Требования по формированию задания на оценку УМЕНИЙ:

-обучающийся должен решать типовые задачи (выполнять задания) на основе воспроизведения стандартных алгоритмов решения;

-применяются следующие средства оценивания компетенций: простые ситуационные задачи (задания) с коротким ответом или простым действием, упражнения, задания на соответствие или на установление правильной последовательности, эссе и другое.

Требования по формированию задания на оценку навыков и (или) ОПЫТА ДЕЯТЕЛЬНОСТИ:

-обучающийся должен решать усложненные задачи (выполнять задания) на основе приобретенных знаний, умений и навыков, с их применением в определенных ситуациях;

-применяются средства оценивания компетенций: задания требующие многошаговых решений как в известной, так и в нестандартной ситуациях, задания, требующие поэтапного решения и развернутого ответа, ситуационные задачи, проектная деятельность, задания расчетно-графического типа. Средства оценивания компетенций выбираются в соответствии с заявленными результатами обучения по дисциплине.

Процедура выставления оценки доводится до сведения обучающихся в течение месяца с начала изучения дисциплиныпутем ознакомления их с технологической картой дисциплины, которая является неотъемлемой частью рабочей учебной программы по дисциплине.

В результате оценивания компетенций на различных этапах их формирования по дисциплине студенту начисляются баллы по шкале, указанной в рабочей учебной программе по дисциплине.

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

Успешность усвоения дисциплиныхарактеризуется качественной оценкой на основе листа оценки сформированности компетенций, который является приложением к зачетно-экзаменационной ведомости при проведении промежуточной аттестации по дисциплине.

Критерии оценивания компетенций

Компетенция считается сформированной, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует *повышенному уровню* сформированности компетенции.

Компетенция считается сформированной, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует *пороговому уровню* сформированности компетенции.

Компетенция считается несформированной, если студентпри выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет практические работы, не демонстрирует необходимых умений, доля

невыполненных заданий, предусмотренных рабочей учебной программой составляет 55 %, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует *допороговому уровню*.

Шкала оценки уровня освоения дисциплины

Качественная оценка может быть выражена: в процентном отношении качества усвоения дисциплины, которая соответствует баллам, и переводится в уровневую шкалу и оценки «отлично» / 5, «хорошо» / 4, «удовлетворительно» / 3, «неудовлетворительно» / 2, «зачтено», «не зачтено». Преподаватель ведет письменный учет текущей успеваемости студента в соответствии с технологической картой по дисциплине.

Шкала оценки результатов освоения дисциплины, сформированности компетенций

Шкалы оценки уровня сформированности компетенции (й)		**Шкала оценки уровня освоения дисциплины**		
Уровневаяшкалаоценкикомпетенций	*100 бальнаяшкала, %*	*100 бальнаяшкала, %*	*5-балльная шкала, дифференцированная оценка/балл*	*недифференцированнаяоценка*
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	незачтено
пороговый	61-85,9	70-85,9	«хорошо» / 4	зачтено
		61-69,9	«удовлетворительно» / 3	зачтено
повышенный	86-100	86-100	«отлично» / 5	зачтено

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Васильков, А. В. Безопасность и управление доступом в информационных системах[Электронный ресурс] : учеб. пособие для сред. проф. образования / А. В. Васильков, И. А. Васильков. - Документ Bookread2. - М. : ФОРУМ [и др.], 2017. - 367 с. : ил., табл. - Режим доступа: http://znanium.com/bookread2.php?book=537054.
2. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты информации[Электронный ресурс] : учеб. для сред. проф. образования по специальности 10.02.01 "Орг. и технология защиты информации" / В. П. Зверева, А. В. Назаров. - Документ Bookread2. - М. : Курс [и др.], 2017. - 317 с. - Режим доступа: http://znanium.com/bookread2.php?book=635130.
3. Эксплуатация объектов сетевой инфраструктуры[Текст] : учеб. для сред. спец. образования по специальности "Компьютер. сети" / А. В. Назаров [и др.] ; под ред. А. В. Назарова. - М. : Академия, 2014. - 368 с. : ил.

Дополнительная литература

4. Защита информации[Электронный ресурс] : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук [и др.]. - 2-е изд. - Документ HTML. - М. : РИОР [и др.], 2015. - 393 с. - Режим доступа: http://znanium.com/bookread.php?book=474838.
5. Каратунова, Н. Г. Защита информации. Курс лекций[Электронный ресурс] : учеб.-метод. пособие / Н. Г. Каратунова ; Кубан. соц.-экон. ин-т, Каф. математики и информатики. -

Документ Bookread2. - Краснодар :Кубан. соц.-экон. ин-т, 2014. - 188 с. - Режим доступа: http://znanium.com/bookread2.php?book=503511.

6. Лабораторный практикум по дисциплине "Защита информации"[Электронный ресурс] : для студентов специальности 230113.51 "Компьютер. системы и комплексы" / Поволж. гос. ун-т сервиса (ФГБОУ ВПО "ПВГУС"), Каф. "Информ. и электрон. сервис" ; сост. Г. П. Жуков. - Документ AdobeAcrobat. - Тольятти : ПВГУС, 2014. - 4,44 МБ, 155 с. - Режим доступа: http://elib.tolgas.ru.

8.2.Перечень ресурсов информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), необходимых для освоения дисциплины

Интернет-ресурсы

1. ИНТУИТ. Национальный Открытый Университет [Электронный ресурс]. - Режим доступа:http://www.intuit.ru/. - Загл. с экрана.
2. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: http://elib.tolgas.ru/. - Загл. с экрана.
3. Электронно-библиотечная система Znanium.com[Электронный ресурс]. - Режим доступа:http://znanium.com/. – Загл. с экрана.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Краткая характеристика применяемого программного обеспечения

№ п/п	Программныйпродукт	Характеристика	Назначение при освоении дисциплины
1	Операционнаясистема Microsoft Windows	MicrosoftWindowsSerwer 2003/2008	*Выполнение и оформление отчета лабораторных работ*
2	Пакет Microsoft Office (MS Word, MS Excel, MS PowerPoint).	Office2003/2007/2010	*Выполнение и оформление отчета лабораторных работ*
3	ПО Антивируса Касперского	ПО Антивируса Касперского	*Выполнение и оформление отчета лабораторных работ*
4	Браузер Internet Explorer		*Выполнение и оформление отчета лабораторных работ*

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

11.Примерная технологическая карта дисциплины ”Защита информации”
Поволжский государственный университет сервиса

кафедра «Информационный и электронный сервис», преподавательЖуков Г.П._ , группа СПКС15_ семестр__5__2017 – 2018уч.года

№	Виды контрольных точек	Кол-во контрольных точек	Количество баллов за 1 контрольную точку	Срок прохождения контрольных точек																
				сентябрь				октябрь					ноябрь				декабрь				Зачетно - экзаменационная сессия
				5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	
				10	17	24	30	8	15	22	29	5	12	19	26	3	10	17	24	31	
I	**Обязательные:**																				
1.1.	Посещение лекций	10	1	+	+		+		+		+		+	+		+		+		+	
1.2.	Вып. лабораторных раб.	8	7				+		+		+		+		+		+		+	+	
1.3.	Промежуточное тестирование	1	5									+									
1.4.	Итоговое тестирование	1	10																+		
	Творческий рейтинг																				
1.5.	Написание творческ. раб.	1	до 5																		
1.6.	Участ.в олимп., конк. и т.д.	1	10																		
1.7.	Индивидуальная работа	1	до 4																		
II.	**Форма контроля**											аттест									зачет