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 междисциплинарному курсу
«Безопасность функционирования информационных систем»
(наименование дисциплины (модуля, междисциплинарного курса))

для студентов специальности 09.02.02 «Компьютерные сети»

Тольятти 2018

Рабочая учебная программа по междисциплинарному курсу «Безопасность функционирования информационных систем» включена в основную профессиональную образовательную программу специальности 09.02.02 «Компьютерные сети» решением Президиума Ученого совета

Протокол № 4 от 28.06.2018 г.

Начальник учебно-методического отдела_____ Н.М.Шемендюк

28.06.2018 г.

Рабочая учебная программа по междисциплинарному курсу разработана в соответствии с Федеральным государственным образовательным стандартом специальности и (или) направления подготовки 09.02.02 «Компьютерные сети», утвержденным приказом Минобрнауки РФ от 28.07.2014 N 803.

Составила: старший преподаватель Васильева А.С.

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

Согласовано начальник учебно-методического отдела _____ Н.М.Шемендюк

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

1.1. Цели освоения междисциплинарного курса

Целью освоения междисциплинарного курса является изучение основных понятий и определений защиты информации; источников риска и форм атак на компьютерную информацию; политики безопасности и законодательно–правовых и организационных методов защиты компьютерной информации; изучение методов и средств организации безопасного функционирования информационных систем.

1.2. Компетенции обучающегося, формируемые в результате освоения междисциплинарного курса

В результате освоения междисциплинарного курса у обучающихся формируются следующие компетенции:

Код компетенции	Наименование компетенции
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности
ПК 3.1	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей
ПК 3.2	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях
ПК 3.3	Эксплуатация сетевых конфигураций
ПК 3.4	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации
ПК 3.5	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта
ПК 3.6	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры

1.3. Перечень планируемых результатов обучения по междисциплинарному курсу

Результаты освоения дисциплины	Технологии формирования компетенции по указанным результатам	Средства и технологии оценки по указанным результатам
Знает: ОК 1-9, ПК 3.1-3.6 архитектуру и функции систем управления сетями, стандарты систем управления; задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией; средства мониторинга и анализа локальных сетей; классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; правила эксплуатации технических средств сетевой инфраструктуры; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры; методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных; основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к	Лекции	Собеседование

архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.		
Умеет: ОК 1-9, ПК 3.1-3.6 выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры; осуществлять диагностику и поиск неисправностей технических средств; выполнять действия по устранению неисправностей в части, касающейся полномочий техника; тестировать кабели и коммуникационные устройства; выполнять замену расходных материалов и мелкий ремонт периферийного оборудования; правильно оформлять техническую документацию; наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных; устанавливать,	Лабораторные работы	Защита лабораторных работ

тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;		
Имеет практический опыт: ОК 1-9, ПК 3.1-3.6 обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя; удаленного администрирования и восстановления работоспособности сетевой инфраструктуры; организации бесперебойной работы системы по резервному копированию и восстановлению информации; поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры;	Лекции Лабораторные работы	Собеседование Защита лабораторных работ

2. Место дисциплины в структуре образовательной программы

Междисциплинарный курс относится к профессиональному модулю «Эксплуатация объектов сетевой инфраструктуры»

Его освоение осуществляется в _____7(оч)/8 (з/о)_____* семестрах.
(указать семестр (ы)

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Код компетенции(й)
	Предшествующие дисциплины	
1	МДК.01.01. Организация, принципы построения и функционирования компьютерных сетей	ОК 1 - 9 ПК 1.1 - 1.5
2	Сетевые технологии CISCO	ПК 1.1 - 1.5
	Последующие дисциплины	
3	Производственная практика (по профилю специальности)	ОК 1 - 9 ПК 1.1 - 1.5, 2.1 - 2.4, 3.1 - 3.6, ПК-4.1

*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 семестрам и видам занятий

Виды занятий	очная форма обучения	заочная форма обучения
Итого часов Зачетных единиц	58	58
Лекции (час)	28	4
Практические (семинарские) занятия (час)	-	-
Лабораторные работы (час)	18	4
Самостоятельная работа (час)	11	49
Курсовой проект (работа) (+,-)	-	-
Контрольная работа (+,-)	-	-
Экзамен, семестр /час.	7	8
Зачет (дифференцированный зачет), семестр	-	-
Контрольная работа, семестр	-	-
Консультации	1ч	1ч

4. Содержание МДК, 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	Практические (семинарские) занятия, час	Лабораторные работы, час	Самостоятельная работа, час	
1	Тема 1. Основные понятия и определения информационной безопасности. 1. Понятия и определения защиты информации и информационной безопасности 2. Угрозы безопасности информационным системам. Технологии обнаружения и предотвращения компьютерной атаки (вторжения) на информацию.	4/2	-	4/0	2/6	Конспект, сообщение, защита лабораторных работ
2	Тема 2. Политика и стандарты безопасности. Законодательно – правовые и организационные	4/0	-	-	2/6	Конспект, опрос на лекции

	методы защиты компьютерной информации. 1. Политика и стандарты безопасности 2. Законодательно – правовые и организационные методы защиты компьютерной информации.					
3	Тема 3. Криптографические модели и методы защиты информации. Алгоритмы шифрования 1. Основные понятия криптологии. Симметричные и асимметричные криптосистемы 2. Классификация методов криптографического преобразования информации 3. Алгоритмы шифрования 4. Электронная цифровая подпись и её применение	6/0	-	8/2	2/11	Конспект, сообщение, защита лабораторных работ
4	Тема 4. Методы и средства защиты информации от несанкционированного доступа. Алгоритмы аутентификации пользователей 1. Способы несанкционированного доступа к информации в компьютерных системах и защиты от него 2. Аутентификация пользователей на основе паролей и модели «рукопожатия» 3. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью 4. Программно-аппаратная защита информации от локального несанкционированного доступа 5.Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях.	4/2	-	2/2	2/10	Конспект, сообщение, защита лабораторных работ
5	Тема 5. Модели безопасности основных ОС. Администрирование сетей. 1. Модели безопасности основных ОС. 2.Администрирование сетей.	6/0	-	-	2/6	Конспект, сообщение, опрос на лекции, защита лабораторных работ

6	Тема 6. Требования к системам защиты информации. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Построение комплексных систем защиты информации. 1. Требования к системам защиты информации 2. Концепция создания защищенных КС. Многоуровневая защита корпоративных сетей. Защита информации в сетях.	4/0	-	4/0	2/10	Конспект, сообщение, защита лабораторных работ
	Промежуточная аттестация по дисциплине	28/4	-	18/4	11/49	Экзамен

4.2. Содержание практических (семинарских) занятий

Практические занятия планом не предусмотрены.

4.3. Содержание лабораторных работ

№	Наименование лабораторных работ	Обьем часов	Наименование темы дисциплины
	7/8 семестр		
1	Лабораторная работа 1. Основные признаки присутствия на компьютере вредоносных программ.	4/0	Основные понятия и определения информационной безопасности.
2	Лабораторная работа 2. Установка и предварительная настройка Антивируса Касперского.	2/2	Методы и средства защиты информации от несанкционированного доступа. Алгоритмы аутентификации пользователей
3	Лабораторная работа 3. Диагностика Антивируса Касперского.	4/0	Требования к системам защиты информации. Многоуровневая защита корпоративных сетей. Защита информации в сетях. Построение комплексных систем защиты информации.
4	Лабораторная работа 4. Количественная оценка стойкости парольной защиты.	2/0	Криптографические модели и методы защиты информации. Алгоритмы шифрования
5	Лабораторная работа 5. Шифрование информации.	2/0	Криптографические модели и методы защиты информации. Алгоритмы шифрования
6	Лабораторная работа 6. Изучение методов шифрования. Шифры замены и шифры перестановки.	4/2	Криптографические модели и методы защиты информации. Алгоритмы

			шифрования
	Итого за семестр	**18/4**	
	Итого	**18/4**	

5. Учебно-методическое обеспечение самостоятельной работы обучающихся по междисциплинарному курсу

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
1	2	3	4	5
ОК 1-9, ПК 3.1-3.6	Выполнение индивидуальных заданий в виде краткого конспекта на заданную тему.	Конспект	Собеседование	5/24
ОК 1-9, ПК 3.1-3.6	Выполнение индивидуальных заданий в виде доклада и презентации на заданную тему.	Доклад, презентация	Собеседование	6/25
			Итого за 7/8 семестр	**11/49**
			Итого	**11/49**

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. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс] : учеб. пособие для сред. проф. образования по группе специальностей "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 416 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=945331.

3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 592 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=937502.

Содержание заданий для самостоятельной работы

Вопросы для самоконтроля

1. Кто в РФ осуществляет Общее руководство системой информационной безопасности осуществляют
2. В каком году был принят закон 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
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.
16. Выполнить проверку носителя информации с помощью Антивируса Касперского
17. 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 / тема лекции	№ практического (семинарского) занятия/наименование темы	№ лабораторной работы / цель
Лекция-дискуссия	-	-	-
Обсуждение проблемной ситуации	-	-	-
Компьютерные симуляции	-	-	-
Деловая (ролевая игра)	-	-	-
Разбор конкретных ситуаций	-	-	№ 1-6
Психологические и иные тренинги	-	-	-
Слайд-лекции	№ 1-6	-	-
Другое *(указать)*	-	-	-

В начале семестра студентам необходимо ознакомиться с технологической картой дисциплины, выяснить, какие результаты освоения дисциплины заявлены (знания, умения, практический опыт). Для успешного освоения дисциплины студентам необходимо выполнить задания, предусмотренные рабочей учебной программой дисциплины и 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 дисциплины учебно-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 с будущей 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 МДК на практических (семинарских) занятиях, лабораторных работах

Практические занятия планом не предусмотрены.

Лабораторные работы

№	Наименование лабораторных работ	Задание по лабораторным работам
1	Основные признаки присутствия на компьютере вредоносных программ.	Задание 1. Изучение настроек браузера Задание 2. Подозрительные процессы Задание 3. Элементы автозапуска Задание 4. Сетевая активность
2	Установка и предварительная настройка Антивируса Касперского.	Задание 1. Системные требования Задание 2. Установка Антивируса Касперского
3	Диагностика Антивируса Касперского.	Задание 1. Тестовый вирус Задание 2. Тестирование с помощью EICAR Задание 3. Лечение инфицированных файлов Задание 4. Помещение файлов на карантин
4	Количественная оценка стойкости парольной защиты.	Рассчитать оценку стойкости парольной защиты.
5	Шифрование информации.	Изучение простейших методов криптографической зашиты информации и закрепление навыков работы в программной среде Microsoft Excel.
6	Изучение методов шифрования. Шифры замены и шифры перестановки.	Научиться применять шифры замены и шифры перестановки для шифрования данных.

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 (письменных работ)

Контрольная работа учебным планом не предусмотрена.

6.3. Методические указания для выполнения курсовых работ (проектов)

Курсового проекта (работы) учебным планом не предусмотрено.

7. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по междисциплинарному курсу (экзамен)

Код оцениваемой компетенции (или ее части)	Тип контроля	Вид контроля	Количество элементов
ОК 1-9, ПК 3.1-3.6	*текущий*	*устный опрос, письменный ответ*	*42-62*
ОК 1-9, ПК 3.1-3.6	*промежуточный*	*тест, письменный ответ*	*1-62*

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

Результаты освоения междисциплинарного курса	**Оценочные средства** (перечень вопросов, заданий и др.)
Знает: ОК 1-9, ПК 3.1-3.6 архитектуру и функции систем управления сетями, стандарты систем управления; задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией; средства мониторинга и анализа локальных сетей; классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; правила эксплуатации технических средств сетевой инфраструктуры; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры; методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных; основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования	1. Защита информации это -: комплекс мероприятий направленных на обеспечение информационной безопасности -: синтез сведений -: анализ и скрытие -: моделирование потоков информации 2. Закон РФ «Об информации, информационных технологиях и о защите информации» принят: -: 2006 году -: 2003 году -: 2004 году -: 2005 году 3. к виду защиты информации относится: -: правовая защита информации -: материальная защита информации -: ЭЦП защита информации -: ГОСТ 26632-85 4. к виду защиты информации относится: -: организационная защита информации -: масштабы защита информации -: электромагнитная защита информации -: лигвинистическая защита информации 5. к виду защиты информации относится: -: инженерно-техническая защита информации -: сопровождение защиты информации -: укрытие защиты информации -: прикладная защита информации 6. Идентификация субъекта — это -: процедура распознавания субъекта

программных средств и баз данных; основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.	-: линия передачи информации -: рабочая среда информации -: человек-техника 7. Аутентификация субъекта — это -: проверка подлинности субъекта -: функции и процедуры -: взаимодействие объекта -: КОБОЛ 8. Субъект доступа к информации — это -: участник правоотношений в информационных процессах -: взаимодействие объекта -: недоступность -: ключ 9. Атака на компьютерную систему — это -: поиск и/или использование злоумышленником той или иной уязвимости системы -: продвижение вируса -: локализация ЭЦП -: физическое уничтожение рабочей станции 10. Защищенная система — это -: система со средствами защиты успешно и эффективно противостоит угрозам безопасности -: системы под электромагитным излучением -: система с аппаратурой -: система с видеонаблюдением 11. По природе возникновения угрозы безопасности информационным системам классифицируют: -: естественные и искусственные -: общепользовательские и индивидуальные -: не правильного ответа -: все правильные ответы 12. Политика безопасности - это -: совокупность норм, правил, рекомендаций регламентирующих работу средств защиты -: для служебного общения -: инструкция поведения объекта -: нет правильных ответов 13. алгоритмы криптографического преобразования информации - это -: все правильные ответы -: простая замена -: гаммирование -: гаммирование с обратной связью 14. Информационная система — это -: совокупность содержащейся в базах данных информации и обеспечивающих ее обработку

информационных технологий и технических средств
-: функции и процедуры
-: взаимодействие объекта
-: КОБОЛ защиты

15. Доступ к информации — это
-: получение субъектом возможности ознакомления с информацией
-: взаимодействие объекта
-: недоступность
-: ключ к информации

16. Доступ к информации различают:
-: санкционированный и несанкционированный
-: только санкционированный
-: локализация ЭЦП
-: только свободный в сети

17. Санкционированный доступ к информации — это
-: доступ не нарушающий установленные правила
-: доступ под электромагитным излучением
-: доступ под контролем ФСБ
-: доступ с видеонаблюдением

18. Несанкционированный доступ к информации характеризуется:
-: нарушением установленных правил разграничения доступа
-: общепользовательский и индивидуальный общественный доступ
-: нет правильного ответа
-: все правильные ответы

19. Ответственным за защиту компьютерной системы от несанкционированного доступа к информации является:
-: администратор защиты
-: директор защиты
-: управляющий защиты
-: нет правильных ответов

20. Законным (легальным) субъектом является:
-: имеющий зарегистрированный идентификатор
-: имеющий пропуск
-: имеющий гаммирование
-: имеющий гаммирование с обратной связью

21. угрозы безопасности ИС по природе возникновения бывают:
-: естественные и искусственные
-: природные
-: техногенные
-: глобальные

22. обнаружение вторжений — это
-: процесс мониторинга событий
-: взаимодействие двух и более объектов
-: обнаружение недоступности
-: глобальная разведка

23. Система обнаружения вторжений - это
-: программный или аппаратный комплекс
-: продвижение вируса
-: локализация объекта
-: физическое видеонаблюдение рабочей станции

24. Общее руководство системой информационной безопасности осуществляют:
-: Президент и Правительство Российской Федерации
-: ФСБ И Президент
-: Дума и Президент
-: совет федерации

25. В РФ какая существует ответственность за неправомерный доступ к компьютерной информации
-: существует уголовная ответственность
-: общественная, управленческая и индивидуальная
-: не существует
-: существует только административная ответственность

26. Статья 272 Уголовного кодекса РФ устанавливает ответственность за:
-: неправомерный доступ к компьютерной информации
-: распространение вредоносных программ для ЭВМ
-: порядка и правил поведения
-: за нарушение правил эксплуатации ЭВМ

27. Статья 273 Уголовного кодекса РФ устанавливает ответственность за:
-: распространение вредоносных программ для ЭВМ
-: порядка и правил поведения
-: за нарушение правил эксплуатации ЭВМ
-: нет правильных ответов

28. Статья 274 Уголовного кодекса РФ устанавливает ответственность за:
-: за нарушение правил эксплуатации ЭВМ
-: нарушение функции и процедуры эксплуатации ПО
-: взаимодействие иностранной агентурой
-: работа на иностранную разведку

29. К аппаратным средствам защиты информации относятся:
-: электронные и электронно-механические устройства

-: задвижки
-: запорные устройства
-: нет правильных ответов

30. Под программными средствами защиты информации понимают:
-: специальные программы
-: продвижение вируса
-: локализация ЭЦП
-: подпрограммы рабочей станции

31. К основным программным средствам защиты информации относятся:
-: программы идентификации и аутентификации
-: программы электромагнитного излучения
-: программы и системы с аппаратурой
-: нет правильных ответов

32. К основным программным средствам защиты информации относятся:
-: программы разграничения доступа пользователей
-: общепользовательские и индивидуальные программы
-: программы раскодирования
-: все правильные ответы

33. К основным программным средствам защиты информации относятся:
-: программы шифрования информации
-: программы для служебного общения с ЭВМ
-: программы индикаторы сообщений
-: нет правильных ответов

34. К основным программным средствам защиты информации относятся:
-: программы защиты информационных ресурсов
-: программа испытания замены
-: подпрограмма гаммирование
-: код программы гаммирования с обратной связью

35. Криптография — это
-: наука, изучающая методы преобразования информации
-: изменения функции и процедуры
-: взаимодействие символов
-: использование цифрового обозначения

36. Какой раздел включает в себя современная криптография
-: симметричные криптосистемы
-: взаимодействие объекта криптографии
-: недоступность криптографии
-: нет правильных ответов

37. Какой раздел включает в себя современная криптография

	-: криптосистемы с открытым ключом -: продвижение криптографии -: локализация криптографии -: физическое уничтожение криптографии 38. Какой раздел включает в себя современная криптография -: системы электронной подписи -: системы под электромагитным излучением -: система с аппаратурой -: система с видеонаблюдением 39. Какой раздел включает в себя современная криптография -: управление ключами -: общепользовательские и индивидуальные криптографии -: нет правильного ответа -: все правильные ответы 40. Под шифрованием понимается: -: процесс зашифрования или расшифрования -: для служебного прослушивания общения -: инструкция поведения объекта информации -: нет правильных ответов 41. Существует ли закон об электронно-цифровой подписи -: существует -: не существует -: это указ Думы -: это инструкция

Умеет: ОК 1-9, ПК 3.1-3.6 выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры; осуществлять диагностику и поиск неисправностей технических средств; выполнять действия по устранению неисправностей в части, касающейся полномочий техника; тестировать кабели и коммуникационные устройства; выполнять замену расходных материалов и мелкий ремонт периферийного оборудования; правильно оформлять техническую документацию; наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных; устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	42. Защита локального компьютера паролем включения: суть, алгоритм настройки, способы преодоления защиты. 43. Защита локального компьютера паролем заставки экрана, суть, алгоритм настройки, способы преодоления защиты. 44. Защита информации скрытием файлов и папок, изменением имени и расширения, атрибутом «только для чтения»: алгоритмы настройки, способы преодоления защиты. 45. MS Office: алгоритмы защиты документов от несанкционированного доступа и использования. Правила задания пароля. Способы преодоления защиты. 46. Особенности строения файлов текстовых процессоров. Алгоритмы уничтожения удалённого и исправленного текста в теле файла текстового процессора. 47. Применение программ-архиваторов для скрытия и защиты файлов. Правила задания пароля. Способы преодоления защиты. 48. Временные файлы, причинны появления временных файлов. Удаление временных файлов программными методами и вкруговую. 49. Программное обеспечение для полного уничтожения удалённых файлов. Алгоритмы работы программ. 50. Алгоритмы настройки защиты дисков, папок, файлов в локальной сети. ПО для защиты компьютера от проникновения из внешней среды. Суть работы программ. 51. Электронная почта: алгоритм отправки сообщении, возможность перехвата, способы защиты. Отправка анонимных сообщений. 52. Опасность программ-апплетов Java, JavaScript. ActiveX. Алгоритмы настройки защиты браузеров. 53. Опасность файлов «cookie». Методы контроле записи файлов «cookie» на жесткий диск. 54. Файловые вирусы: наиболее общий алгоритм работы, алгоритм обнаружения вирусов, возможность восстановления файлов. 55. Загрузочный вирус, алгоритм получения управления вирусом. Алгоритмы предотвращения заражения, обнаружения заражения, удаления вируса. 56. Макровирусы, принципы устройства и функционирования. Алгоритмы обнаружения вирусов и обезвреживания файлов.
Имеет практический опыт: ОК 1-9, ПК 3.1-3.6 обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя; удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;	Выполнение лабораторных работ: 57. Основные признаки присутствия на компьютере вредоносных программ. 58. Установка и предварительная настройка Антивируса Касперского. 59. Диагностика Антивируса Касперского. 60. Количественная оценка стойкости парольной

организации бесперебойной работы системы по резервному копированию и восстановлению информации; поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры;	защиты. 61. Шифрование информации. 62. Изучение методов шифрования. Шифры замены и шифры перестановки.

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

Рабочая учебная программа дисциплины содержит следующие структурные элементы:

- перечень компетенций, формируемых в результате изучения дисциплины в процессе освоения образовательной программы;

- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности 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 дисциплины и 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 дисциплины путем ознакомления их с технологической картой дисциплины, которая является неотъемлемой частью рабочей учебной программы по дисциплине.

В результате оценивания компетенций по дисциплине студенту начисляются баллы по шкале, указанной в рабочей учебной программе по дисциплине.

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Успешность усвоения дисциплины характеризуется 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 студент при 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 междисциплинарного курса

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 междисциплинарного курса, сформированности компетенций

Шкалы оценки уровня сформированности компетенции (й)		**Шкала оценки уровня освоения дисциплины**		
Уровневая шкала оценки компетенций	*100 бальная шкала, %*	*100 бальная шкала, %*	*5-балльная шкала, дифференцированная оценка/балл*	*недифференцированная оценка*
допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	Не зачтено
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 междисциплинарного курса

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

Списки основной литературы

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. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс] : учеб. пособие для сред. проф. образования по группе специальностей "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 416 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=945331.

3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : учеб. пособие для вузов по направлению 09.03.01 "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ Bookread2. - М. : ФОРУМ [и др.], 2018. - 592 с. : ил. - Режим доступа: http://znanium.com/bookread2.php?book=937502.

Списки дополнительной литературы

4. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры [Электронный ресурс] : учеб. для проф. образоват. орг. по специальности 09.02.02 "Компьютер. сети" / А. В. Назаров, А. Н. Енгалычев, В. П. Мельников. - Документ Bookread2. - М. : Курс [и др.], 2017. - 360 с. - Режим доступа: http://znanium.com/bookread2.php?book=635086.

5. Олифер, В. Г. Безопасность компьютерных сетей [Текст] / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия -Телеком, 2016. - 644 с. : ил.

6. 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.

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. Образовательные ресурсы Интернета. Информатика [Электронный ресурс]. - Режим доступа: http://www.alleng.ru/edu/comp.htm. - Загл. с экрана.
3. Электронная библиотека. Техническая литература [Электронный ресурс]. - Режим доступа: http://techliter.ru/. – Загл. с экрана.
4. Электронная библиотечная система Поволжского государственного университета сервиса [Электронный ресурс]. - Режим доступа: http://elib.tolgas.ru/. - Загл. с экрана.
5. 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 МДК, включая перечень программного обеспечения и информационных справочных систем

Краткая характеристика применяемого программного обеспечения

№ п/п	Программный продукт	Характеристика	Назначение при освоении дисциплины
1	Операционная система Microsoft Windows	Windows — семейство коммерческих операционных систем (ОС) корпорации Microsoft, ориентированных на применение графического интерфейса при управлении.	Выполнение лабораторных работ и оформление отчетов по ним
2	Пакет Microsoft Office (MS Word, MS	Офисный пакет приложений, созданных корпорацией Microsoft для операционных систем Microsoft Windows, Windows Phone, Android, OS X, iOS. В состав этого пакета	Выполнение лабораторных работ и оформление отчетов по ним

	Excel, MS PowerPoint).	входит программное обеспечение для работы с различными типами документов: текстами, электронными таблицами, базами данных и др.	
3	ПО Антивирус Касперского	Антивирус Касперского — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского.	Выполнение лабораторных работ и оформление отчетов по ним
4	Mozilla Firefox	Mozilla Firefox — свободный браузер на движке Gecko, разработкой и распространением которого занимается Mozilla Corporation.	Выполнение лабораторных работ и оформление отчетов по ним

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

Реализация программы дисциплины в соответствии с требованиями ФГОС СПО по специальности требует наличие учебного кабинета, укомплектованного специализированной мебелью, техническими средствами обучения, и лаборатории программно-аппаратной защиты объектов сетевой инфраструктуры, оснащенной лабораторным оборудованием различной степени сложности

11. Примерная технологическая карта междисциплинарного курса «Безопасность функционирования информационных систем»

Институт (факультет) СПО
кафедра «Информационный и электронный сервис»
преподаватель Васильева А.С., специальность 09.02.02 «Компьютерные сети»

№	Виды контрольных точек	Кол-во контр. точек	Кол-во баллов за 1 контр. точку	График прохождения контрольных точек																зач. неделя
				Сентябрь (февраль)				Октябрь (март)				Ноябрь (апрель)				Декабрь (май)				
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1	**Обязательные:**																			
1.1	Посещение лекционных занятий	14	1		+	+	+	+	+	+	+	+	+	+	+	+	+	+		
1.2	Защита лабораторных работ	6	7				+		+		+		+		+		+			
1.3	Промежуточное тестирование	1	15								+									
1.4	Итоговое тестирование	1	15															+		
2	**Творческий рейтинг:**																			
2.1	Участие в студенческих конференциях	1	7						+											
2.2	Участие в олимпиадах	1	7														+			
	Экзамен																			+