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 ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА

МДК.03.02 «БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»

Специальность 09.02.06 «Сетевое и системное администрирование»

Тольятти 2020

Рабочая программа междисциплинарного курса «Безопасность компьютерных сетей» разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование», утверждённым приказом Министерства образования и науки от 9 декабря 2016 года № 1548.

Разработчик РПД:

Ассистент		К.В. Ляпина
(ученая степень, ученое звание)	(подпись)	(ФИО)

СОГЛАСОВАНО:

Директор научной библиотеки _____ (подпись) В.Н.Еремина

Начальник управления по информатизации _____ (подпись) В.В.Обухов

РПД утверждена на заседании кафедры «Информационный и электронный сервис»
« 27 » декабря 20 19 г., протокол № 5

Заведующий кафедрой,	д.т.н., профессор		В.И. Воловач
	(уч.степень, уч.звание)	(подпись)	(ФИО)

СОГЛАСОВАНО:

Начальник учебно-методического отдела _____ (подпись) Н.М.Шемендюк

Рабочая программа дисциплины утверждена в составе основной профессиональной образовательной программы решением Ученого совета Протокол № 4 от 22.01.2020 г.

Рабочая программа дисциплины актуализирована и утверждена в составе образовательной программы решением Ученого совета от 23.09.2020 г. Протокол №3

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО МДК, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения МДК

Целью освоения междисциплинарного курса является формирование у обучающихся следующих компетенций:

Код компетенции	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
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	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации
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.

1.2. Планируемые результаты освоения МДК

В результате освоения междисциплинарного курса обучающийся должен:

иметь практический опыт:

обслуживать сетевую инфраструктуру, восстанавливать работоспособность сети после сбоя;
удаленно администрировать и восстанавливать работоспособность се- тевой инфраструктуры;
поддерживать пользователей сети, настраивать аппаратное и про- граммного обеспечения сетевой инфраструктуры.

уметь:

выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
осуществлять диагностику и поиск неисправностей всех компонентов сети;
выполнять действия по устранению неисправностей.

знать:

архитектуру и функции систем управления сетями, стандарты систем управления;
средства мониторинга и анализа локальных сетей;
методы устранения неисправностей в технических средствах.

1.3. Место МДК в структуре образовательной программы

Междисциплинарный курс «Безопасность компьютерных сетей» относится к модулю ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» основной профессиональной образовательной программы.

2. СТРУКТУРА И СОДЕРЖАНИЕ МДК

2.1. Объём учебной междисциплинарного курса и виды учебной работы

Общая трудоёмкость МДК составляет **110 часов.** Их распределение по видам работ представлено в таблице:

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины	**110**
Объем работы обучающихся во взаимодействии с преподавателем по видам учебных занятий (всего), в т.ч.:	**84**
лекции	**34**
лабораторные работы	**22**
практические занятия	**26**
курсовое проектирование (консультации)	
Самостоятельная работа	**26**
Контроль (часы на экзамен, зачет, контрольную работу)	**2**
Консультация перед экзаменом	
Промежуточная аттестация	**дифференцированный зачет**

2.2. Содержание МДК, структурированное по темам, для студентов ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ

Коды компетенций, формированию которых способствует элемент программы	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Работа во взаимодействии с преподавателем			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
6 семестр						
ОК.01-ОК.04, ОК.09, ОК.10, ПК.3.1-ПК.3.6	**Тема 1. Безопасность компьютерных сетей** Содержание темы: **1. Фундаментальные принципы безопасной сети** Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак. **2. Безопасность Сетевых устройств OSI** Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности. **3. Авторизация, аутентификация и учет доступа (AAA)** Свойства AAA. Локальная AAA аутентификация. Server-based AAA **4. Реализация технологий брандмауэра** ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основан-ные на зонах. **5. Реализация технологий предотвращения вторжения** IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS **6. Безопасность локальной сети** Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN **7. Криптографические системы** Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей. 8 Реализация технологий VPN VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN с исполь-зованием CLI. Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN **9. Управление безопасной сетью** Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварий-ных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик без-опасности.	34				*Тестирование*

Коды компетенций, формированию которых способствует элемент программы	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Работа во взаимодействии с преподавателем			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОК.01-ОК.04, ОК.09, ОК.10, ПК.3.1-ПК.36	**10. Cisco ASA** Введение в Адаптивное устройство безопасности ASA. Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.					*Защита лабораторных и практических работ*
	Лабораторная работа № 1 Социальная инженерия		2			
	Практическое занятие № 1 Исследование сетевых атак и инструментов проверки защиты сети			2		
	Лабораторная работа № 2 Настройка безопасного доступа к маршрутизатору		2			
	Практическое занятие № 2 Обеспечение административного доступа AAA и сервера Radius			4		
	Лабораторная работа № 3 Настройка политики безопасности брандмауэров		2			
	Практическое занятие № 3 Настройка системы предотвращения вторжений (IPS)			4		
	Лабораторная работа № 4 Настройка безопасности на втором уровне на коммутаторах		2			
	Практическое занятие № 4 Исследование методов шифрования			4		
	Лабораторная работа № 5 Настройка Site-to-SiteVPN используя интерфейс командной строки		2			
	Практическое занятие № 5 Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки			4		
	Лабораторная работа № 6 Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM		4			
	Практическое занятие № 6 Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM			4		
	Лабораторная работа № 7 НастройкаClientless Remote Access SSL VPNs используя ASDM		4			
	Практическое занятие № 7 Настройка AnyConnect Remote Access SSL VPN используя ASDM			4		
	Лабораторная работа № 8 Финальная комплексная лабораторная работа по безопасности		4			
	Самостоятельная работа обучающихся : 1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы. 2. Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа при самом широком использовании Интернета и других IT-технологий. 3. Проектные формы работы, подготовка сообщений к выступлению на семинарах и конференциях; подготовка рефератов, докладов.				26	

Коды компетенций, формированию которых способствует элемент программы	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Работа во взаимодействии с преподавателем			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОК.01-ОК.04, ОК.09, ОК.10, ПК.3.1-ПК.3.6	4. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите.					
	ИТОГО за 6 семестр	**34**	**22**	**26**	**26**	

2.3. Формы и критерии текущего контроля успеваемости (технологическая карта для студентов очной формы обучения)

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Отчет по практической работе	7	4	28
Отчет по лабораторной работе	8	4	32
Тестирование	1	30	30
Творческий рейтинг (заочное участие в конференциях, научные статьи и т.п.)	1	10	10
		Итого по семестру	**100 баллов**

2.4. Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Условия допуска	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
		Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
дифференцированный зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования)	допускаются все студенты	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
		пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
				70-85,9	«хорошо» / 4	зачтено
		повышенный	86-100	86-100	«отлично» / 5	зачтено

3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ МДК

3.1. Общие методические рекомендации по освоению МДК, образовательные технологии

МДК реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

Контактная работа может быть аудиторной, внеаудиторной, а также проводиться в электронной информационно-образовательной среде университета (далее - ЭИОС). В случае проведения части контактной работы по дисциплине в ЭИОС (в соответствии с расписанием учебных занятий), трудоемкость контактной работа в ЭИОС эквивалентна аудиторной работе.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- балльно-рейтинговая технология оценивания;
- электронное обучение.

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами. Студентам, набравшим в ходе текущего контроля успеваемости по МДК от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения МДК.

Результат обучения считается сформированным (повышенный уровень), 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 результатов обучения.

Результат обучения считается сформированным (пороговый уровень), 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 результатов обучения.

Результат обучения считается несформированным, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с

большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

3.2. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 4.

В процессе самостоятельной работы при изучении дисциплины студенты могут использовать в специализированных аудиториях для самостоятельной работы компьютеры, обеспечивающему доступ к программному обеспечению, необходимому для изучения дисциплины, а также доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении МДК.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

3.3. Методические указания для выполнения курсового проекта / работы

Выполнение курсового проекта/ работы учебным планом не предусмотрено.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ МДК

4.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения МДК

Основная литература:

1. Баранова, Е. К. Основы информационной безопасности [Электронный ресурс] : учебник / Е. К. Баранова, А. В. Бабаш. - Документ Bookread2. - М. : Риор [и др.], 2019. - 202 с. - Режим доступа: http://znanium.com/bookread2.php?book=1014830.
2. 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. - Режим доступа: http://znanium.com/bookread2.php?book=537054.
3. 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.
4. 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.

Дополнительная литература:

5. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс] : учеб. пособие для вузов по направлениям подгот. 09.03.03 "Приклад. информатика" и 10.03.01 "Информ. безопасность" / Е. В. Глинская, Н. В. Чичварин. - Документ Bookread2. - М. : ИНФРА-М, 2018. - 117 с. - Режим доступа: http://znanium.com/bookread2.php?book=925825.
6. Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова. - Изд. 2-е, испр. - Документ Reader. - СПб. : Лань, 2020. - 124 с. - Режим доступа: https://e.lanbook.com/reader/book/133924/#1.

4.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. КонсультантПлюс [Электронный ресурс]: Справочная правовая система. - Режим доступа: http://www.consultant.ru/.
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.
4. Электронно-библиотечная система «Издательство Лань» [Электронный ресурс]. - Режим доступа: https://e.lanbook.com/. – Загл. с экрана.
5. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. - Режим доступа: http://elibrary.ru/defaultx.asp. - Загл с экрана.

4.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)

5. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МДК)

Специальные помещения представляют собой учебные аудитории для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных стандартов.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа *(при наличии в учебном плане)*. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Лабораторные работы *(при наличии в учебном плане)*. Для проведения лабораторных работ используется учебная аудитория «Лаборатория эксплуатации объектов сетевой инфраструктуры», оснащенная следующим оборудованием:

- 12-15 компьютеров обучающихся и 1 компьютер преподавателя (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i3, оперативная память объемом не менее 8 Гб; HD 500 Gb или больше программное обеспечение: операционные системы Windows, UNIX, пакет офисных программ, пакет САПР);
- Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ-45, тестеры для кабеля, кросс-ножи, кросс-панели;
- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности
- Сервер в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 8-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 2 Тб, программное обеспечение: Windows Server 2012 или более новая версия, лицензионные антивирусные программы, лицензионные программы восстановления данных, лицензионный программы по виртуализации.)
- Технические средства обучения:
- Компьютеры с лицензионным программным обеспечением
- Интерактивная доска
- Проектор

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интеренет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

компьютерные классы университета;

библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

6. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости

Типовые задания к практическим (семинарским) занятиям

Практическое занятие № 1. Исследование сетевых атак и инструментов проверки защиты сети.
Задание.
• Изучение методики исследования сетевых атак и инструментов проверки защиты сети;
• Выполнение исследования сетевых атак и инструментов проверки защиты сети;
• Отчет о проделанной работе.

Практическое занятие № 2. Обеспечение административного доступа AAA и сервера Radius.
Задание.
• Изучение методики обеспечения административного доступа AAA и сервера Radius;
• Выполнение работы по обеспечению административного доступа AAA и сервера Radius;
• Отчет о проделанной работе.

Практическое занятие № 3. Настройка системы предотвращения вторжений (IPS).
Задание.
• Изучение методики настройки системы предотвращения вторжений (IPS);
• Выполнение настройки;
• Отчет о проделанной работе.

Практическое занятие № 4. Исследование методов шифрования
Задание.
Изучить возможности методов шифрования заменой:
1 омофоническим шифром;
2 по таблице Виженера.
3. Составить таблицу омофонического шифра
4. Зашифровать заменой свои Ф.И.О. омофоническим шифром.
5. Составить таблицу Вижинера.
6. Зашифровать заменой свои Ф.И.О. по таблице Виженера.

Практическое занятие № 5. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки.
Задание.
• Изучение методики базовой настройки шлюза безопасности ASA и настройки брандмауэров используя интерфейс командной строки;
• Выполнение настройки;
• Отчет о проделанной работе.

Практическое занятие № 6. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.
Задание.
• Изучение методики настройки Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM;
• Выполнение настройки;
• Отчет о проделанной работе.

Практическое занятие № 7. Настройка AnyConnect Remote Access SSL VPN используя ASDM.

Задание.
• Изучение методики настройки AnyConnect Remote Access SSL VPN используя ASDM;
• Выполнение настройки;
• Отчет о проделанной работе.

Типовые задания для лабораторных работ

Лабораторная работа № 1. Социальная инженерия.
Задание
1. Сделать презентацию терминов, указанных в задании
2. Выполнить анализ объекта защиты информации по предложенным выше пунктам:
А) Описать автоматизированную информационную систему для предложенного преподавателем виртуального предприятия (указать составляющие автоматизированной системы, их основные характеристики и т.д.)
Б) Предположить угрозы и уязвимости для этой системы
В) Указать технологии, средства и инструменты, которые можно применить для защиты информации в автоматизированной системе указанного объекта.
Г) Предположить возможные действия нарушителей при условии выполнения защиты информации в соответствии с п. В)
3. Разработать документ «Политика безопасности», указать СПИСОК документов, которые необходимо разработать для реализации политики безопасности на предприятии.
4. Составить тест (или кроссворд), включающий не менее 10 терминов (или основных понятий) курса (тест должен содержать не менее 3-х вариантов ответа).
5. Результаты работы оформить в виде отчета (текстовый файл, файл - презентация). Отчет должен содержать ФИО студента, номер группы, ответы на поставленные вопросы. Название папки должно содержать фамилию и группу студента.

Лабораторная работа № 2. Настройка безопасного доступа к маршрутизатору.
Задание
• Изучение методики настройки настройка безопасного доступа к маршрутизатору;
• Выполнение настройки;
• Отчет о проделанной работе.

Лабораторная работа № 3. Настройка политики безопасности брандмауэров.
Задание
• Изучение методики настройки политики безопасности брандмауэров;
• Выполнение настройки;
• Отчет о проделанной работе.

Лабораторная работа № 4. Настройка безопасности на втором уровне на коммутаторах.
Задание.
• Изучение методики настройки настройки безопасности на втором уровне на коммутаторах;
• Выполнение настройки;
• Отчет о проделанной работе.
.

Лабораторная работа № 5. Настройка Site-to-SiteVPN используя интерфейс командной строки.
Задание
• Изучение методики настройки Site-to-SiteVPN используя интерфейс командной строки;
• Выполнение настройки;
• Отчет о проделанной работе.

Лабораторная работа № 6. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM.
Задание
• Изучение методики базовой настройки шлюза безопасности ASA и настройки брандмауэров используя ASDM;
• Выполнение настройки;
• Отчет о проделанной работе.
.
Лабораторная работа № 7. НастройкаClientless Remote Access SSL VPNs используя ASDM.
Задание
• Изучение методики настройки Clientless Remote Access SSL VPNs используя ASDM;
• Выполнение настройки;
• Отчет о проделанной работе.

Лабораторная работа № 8
Финальная комплексная лабораторная работа по безопасности
Задание
• Изучение методики комплексной оценки безопасности;
• Комплексная оценка безопасности;
• Отчет о проделанной работе.

7.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации

Форма проведения промежуточной аттестации по МДК: *дифференцированный зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).*

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

Перечень вопросов и заданий для подготовки к дифференцированному зачету

ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6:

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.

Примерный тест для итогового тестирования

ОК 01, ОК 02, ОК 03, ОК 04, ОК 09, ОК 10, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6:

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
-: 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

Регламент проведения промежуточной аттестации в форме компьютерного тестирования

Кол-во заданий в банке вопросов	Кол-во заданий, предъявляемых студенту	Время на тестирование, мин.
не менее 100 или указывается конкретное количество тестовых заданий	*30*	*30*

Полный фон оценочных средств для проведения промежуточной аттестации в форме компьютерного тестирования размещен в банке вопросов данного курса дисциплины в ЭИОС университета http://sdo.tolgas.ru/.

В ходе подготовки к промежуточной аттестации обучающимся предоставляется возможность пройти тест самопроверки. Тест для самопроверки по дисциплине размещен в ЭИОС университета http://sdo.tolgas.ru/ в свободном для студентов доступе.

АННОТАЦИЯ

МДК.03.02 «Безопасность компьютерных сетей»

Междисциплинарный курс «Безопасность компьютерных сетей» относится к модулю ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» основной профессиональной образовательной программы.

Целью освоения междисциплинарного курса является формирование у обучающихся следующих компетенций:

Код компетенции	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
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	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации
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.

В результате освоения междисциплинарного курса обучающийся должен:

иметь практический опыт:

обслуживать сетевую инфраструктуру, восстанавливать работоспособность сети после сбоя;
удаленно администрировать и восстанавливать работоспособность се- тевой инфраструктуры;
поддерживать пользователей сети, настраивать аппаратное и про- граммного обеспечения сетевой инфраструктуры.

уметь:

выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
осуществлять диагностику и поиск неисправностей всех компонентов сети;
выполнять действия по устранению неисправностей.

знать:

архитектуру и функции систем управления сетями, стандарты систем управления;
средства мониторинга и анализа локальных сетей;
методы устранения неисправностей в технических средствах.