

Документ подписан простой электронной подписью
Информация о лице:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 26.09.2024
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Колледж креативных индустрий и предпринимательства

РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА
МДК.03.02 «БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ»

Специальность
09.02.06 «Сетевое и системное администрирование»

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», утвержденным приказом Министерства образования и науки Российской Федерации от 10 июля 2023 года № 519.

Разработчик РПД:

преподаватель
(ученая степень, ученое звание)

А.К. Попов
(ФИО)

Рассмотрена на заседании предметно-цикловой комиссии по образовательной программе 09.02.06 Сетевое и системное администрирование

Протокол от «22» ноября 2024 г., № 3

Председатель ПЦК

О.Г. Седнев, преподаватель
(ФИО, должность, ученая степень, ученое звание)

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

1.1. Цель освоения МДК

Целью освоения МДК является формирование у обучающихся следующих компетенций:

Код компетенции	Наименование компетенции
ПК 3.1	Осуществлять проектирование сетевой инфраструктуры
ПК 3.3	Осуществлять защиту информации в сети с использованием программно-аппаратных средств
ПК 3.5	Модернизировать сетевые устройства информационно-коммуникационных систем

1.2. Планируемые результаты освоения МДК

В результате освоения МДК обучающийся должен:

иметь практический опыт:

- обслуживать сетевую инфраструктуру, восстанавливать работоспособность сети после сбоя;
- удаленно администрировать и восстанавливать работоспособность сетевой инфраструктуры;
- поддерживать пользователей сети, настраивать аппаратное и программное 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 профессиональному циклу ПМ.03 Эксплуатация объектов сетевой инфраструктуры основной профессиональной образовательной программы.

2. СТРУКТУРА И СОДЕРЖАНИЕ МДК

2.1. Объем МДК и виды учебной работы

Общая трудоёмкость МДК составляет **64 часа**. Их распределение по видам работ представлено в таблице:

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость МДК	64
Объем работы обучающихся во взаимодействии с преподавателем по видам учебных занятий (всего), в т.ч.:	60
лекции	20
лабораторные работы	16
практические занятия	24
Самостоятельная работа	2
Контроль (часы на контрольную работу)	2
Консультация перед экзаменом	-
Промежуточная аттестация	Дифференцированный зачет

2.2. Содержание МДК, структурированное по темам.

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		
ПК 3.1, ПК 3.3, ПК 3.5	Тема 1. Проблемы информационной безопасности компьютерных сетей. Содержание темы: - 1.Модель ISO/OSI и стек протоколов TCP/IP как основной стандарт построения компьютерных сетей - 2.Угрозы сетевой безопасности и проблемы безопасности IP-сетей - 3.Угрозы безопасности беспроводным сетям и уязвимости беспроводных сетей - 4.Обеспечение информационной безопасности компьютерных сетей	3				Конспектирование лекционного материала
	Самостоятельная работа: поиск материала по теме.					
ПК 3.1, ПК 3.3, ПК 3.5	Тема 2. Криптографическая защита информации в компьютерных сетях. Содержание темы: - 1.Основные понятия криптографической защиты информации - 2.Симметричные криптосистемы шифрования - 3.Асимметричные криптосистемы шифрования - 4.Функция хэширования - 5.Электронная цифровая подпись	4				Конспектирование лекционного материала Отчет по лабораторным работам
	Лабораторная работа №1. Оценка устойчивости паролей и алгоритмов шифрования		4			
	Лабораторная работа №2. Исследование методов шифрования: шифры замены и перестановки		4			
	Самостоятельная работа: подготовка к лабораторным работам, поиск материала по теме.					
ПК 3.1, ПК 3.3, ПК 3.5	Тема 3. Идентификация, аутентификация и управление доступом Содержание темы: - 1.Аутентификация, авторизация и администрирование действий пользователей в компьютерных сетях - 2.Аутентификация на основе многоразовых паролей	4				Конспектирование лекционного материала Отчет по практическим заданиям

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		
	- 3.Аутентификация на основе одноразовых паролей - 4.Биометрическая аутентификация пользователей					
	Практическая работа №1. Аппаратно-программные средства защиты информации в компьютерных системах			6		
	Самостоятельная работа: подготовка к практическим работам, поиск материала по теме.				1	
ПК 3.1, ПК 3.3, ПК 3.5	Тема 4.Безопасность операционных систем Содержание темы: - 1.Угрозы безопасности операционной системы - 2.Понятие защищенной операционной системы	3				Конспектирование лекционного материала Отчет по практическим заданиям
	Практическая работа №2. Организация безопасного обмена трафиком в сети			6		
	Самостоятельная работа: подготовка к практическим работам, поиск материала по теме.					
ПК 3.1, ПК 3.3, ПК 3.5	Тема 5. Современные подходы к обеспечению анонимности работы в сети Интернет Содержание темы: - 1.Прокси-серверы - 2.Виртуальные частные сети (VPN/SSH) - 3.Сеть анонимизации TOR - 4.Сеть анонимизации I2P	3				Конспектирование лекционного материала Отчет по лабораторным работам
	Лабораторная работа №3. Проверка целостности данных с использованием хеш-функций		4			
	Лабораторная работа №4. Применение шифрования для защиты файлов		4			
	Самостоятельная работа: подготовка к лабораторным работам, поиск материала по теме.				1	
ПК 3.1, ПК 3.3, ПК 3.5	Тема 6. Вредоносные программы и спам Содержание темы: - 1.Классификация вредоносных программ - 2.Рекомендации по безопасной работе в сети Интернет	3				Конспектирование лекционного материала Отчет по практическим заданиям

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		
	Практическая работа №3. Защита беспроводных сетей Wi-Fi			6		
	Практическая работа №4. Настройка и использование ACL-списков для контроля доступа в сети			6		
	ИТОГО	20	16	24	2	

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
Конспектирование лекционного материала	7	4	28
Отчет по лабораторным работам	4	9	36
Отчет по практическим заданиям	4	9	36
Итого по МДК			100 баллов

2.4. Шкала оценки результатов освоения МДК, сформированности результатов обучения

Форма проведения промежуточной аттестации	Условия допуска	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения МДК		
		Уровневая шкала оценки компетенций	100 балльная шкала, %	100 балльная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Дифференцированный зачет (по накопительному рейтингу или компьютерное тестирование)	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 МДК в ЭИОС (в соответствии с расписанием учебных занятий), трудоемкость контактной работа в ЭИОС эквивалентна аудиторной работе.

При проведении учебных занятий по МДК 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 МДК 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 МДК ведется с применением следующих видов образовательных технологий:

- *балльно-рейтинговая технология оценивания;*
- *электронное обучение;*
- *репродуктивные технологии;*
- *технологии развивающего обучения;*
- *практико-ориентированные технологии.*

Для оценки знаний, умений, навыков и уровня сформированности компетенции по МДК 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 изучаемому МДК. 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 МДК студенты могут использовать в специализированных аудиториях для самостоятельной работы компьютеры, обеспечивающему доступ к программному обеспечению, необходимому для изучения МДК, 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.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ МДК

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

Основная литература:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие для сред. проф. образования по группе специальностей "Информатика и вычисл. техника" / В. Ф. Шаньгин. - Документ read. - Москва : ФОРУМ [и др.], 2023. - 416 с. : ил. - (Среднее профессиональное образование). - Прил. - URL: <https://znanium.ru/read?id=418929> (дата обращения: 17.01.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8199-0754-2. - 978-5-16-101207-9. - Текст : электронный.
2. Васильков, А. В. Безопасность и управление доступом в информационных системах : учеб. пособие для сред. проф. образования / А. В. Васильков, И. А. Васильков. - Документ read. - Москва : ФОРУМ [и др.], 2022. - 367 с. : ил., табл. - (Среднее профессиональное образование). - Предм. указ. - URL: <https://znanium.ru/read?id=399436> (дата обращения: 14.03.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-91134-360-6. - 978-5-16-012933-4. - 978-5-16-104336-3. - Текст : электронный.
3. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учеб. для проф. образоват. орг. по специальности 09.02.02 "Компьютер. сети" / А. В. Назаров, А. Н. Енгальчев, В. П. Мельников. - Документ Bookread2. - Москва : Курс [и др.], 2023. - 360 с. - (Среднее профессиональное образование) (Среднее профессиональное образование). - URL: <https://znanium.ru/read?id=428836> (дата обращения: 17.01.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-906923-06-6. - 978-5-16-105198-6. - Текст : электронный.
4. Баранова, Е. К. Основы информационной безопасности : учебник / Е. К. Баранова, А. В. Бабаш. - Документ read. - Москва : Риор [и др.], 2022. - 202 с. - (Среднее профессиональное образование). - Варианты итог. тест. заданий. - Слов. терминов. - URL: <https://znanium.com/read?id=393455> (дата обращения: 25.02.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-369-01806-4. - 978-5-16-107531-9. - Текст : электронный.

Дополнительная литература:

1. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие для вузов по направлениям подгот. 09.03.03 "Приклад. информатика" и 10.03.01 "Информ. безопасность" (квалификация (степень) "бакалавр") / Е. В. Глинская, Н. В. Чичварин. - Документ read. - Москва : ИНФРА-М, 2021. - 118 с. - (Высшее образование - Бакалавриат). - Прил. - URL: <https://znanium.com/read?id=362430> (дата обращения: 12.04.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-16-102993-0. - Текст : электронный.
2. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. - Изд. 4-е, стер. - Документ Reader. - Санкт-Петербург : Лань, 2022. - 124 с. - (Учебники для вузов. Специальная литература). - URL: <https://reader.lanbook.com/book/217445> (дата обращения: 06.10.2022). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-44201-0. - Текст : электронный.

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

1. eLIBRARY.RU : научная электронная библиотека : сайт. - Москва, 2000 - . - URL : <https://elibrary.ru> (дата обращения: 03.12.2021). - Режим доступа: для зарегистрир. пользователей. - Текст: электронный.
2. Единое окно доступа к образовательным ресурсам : сайт. - URL : <http://window.edu.ru/> (дата обращения: 03.12.2021). - Текст : электронный.
3. Университетская информационная система РОССИЯ : сайт. - URL : <http://uisrussia.msu.ru> (дата обращения: 03.12.2021). - Текст : электронный.
4. Федеральная служба государственной статистики : сайт. - Москва, 1999 - . - URL: <http://www.gks.ru/> (дата обращения: 03.12.2021). - Текст: электронный.

5. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL : <http://elib.tolgas.ru> (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.

6. Электронно-библиотечная система Znanium.com : сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . – URL : <https://znanium.com/> (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.

7. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: <https://e.lanbook.com/> (дата обращения 03.12.2021). - Режим доступа: для авториз. пользователей. - Текст : электронный.

4.3. Программное обеспечение

Информационное обеспечение учебного процесса по междисциплинарному курсу 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 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 МДК.

Занятия семинарского типа. Для проведения практических занятий используется учебная аудитория, укомплектованная мебелью и техническими средствами обучения, служащими для представления учебной информации (переносной набор демонстрационного оборудования (проектор, экран, /ноутбук).

Лабораторные работы. Для проведения лабораторных работ используется учебная аудитория «Лаборатория информационных технологий, информатики и методов программирования (Г-413)», оснащённая следующим оборудованием: Компьютер Аксус Intel G530\iH61\GeForceGT430\4096 Mb DDR3\500Gb\LCD 22" - 14 шт., Компьютер в сборе iP2.0 LCD - 1 шт., принтер HP 1200 - 1 шт., мобильный экран проекционный Draper Luma - 1 шт., мобильный проектор Sanyo PLC, Сетевое оборудование D-Link DES-1024D, 24-портовый; локальная сеть 100 мб с доступом в Интернет 50 мб.

Промежуточная аттестация. Для проведения промежуточной аттестации по МДК 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 «Интернет» 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 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).

К предметным результатам освоения МДК дополнительно относятся:

- 1) для слепых, слабовидящих обучающихся:
 - сформированность навыков письма на брайлевской печатной машинке;
- 2) для глухих, слабослышащих, позднооглохших обучающихся:
 - сформированность и развитие основных видов речевой деятельности обучающихся - слухозрительного восприятия (с использованием слуховых аппаратов и (или) кохлеарных имплантов), говорения, чтения, письма;
- 3) для обучающихся с расстройствами аутистического спектра:
 - овладение основными стилистическими ресурсами лексики и фразеологии языка, основными нормами литературного языка, нормами речевого этикета; приобретение опыта их использования в речевой и альтернативной коммуникативной практике при создании устных, письменных, альтернативных высказываний; стремление к возможности выразить собственные мысли и чувства, обозначить собственную позицию.

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

7.1.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа №1. Аппаратно-программные средства защиты информации в компьютерных системах. Цель: изучить аппаратно-программные средства защиты информации в современных компьютерных системах. Задание: настроить и протестировать различные средства защиты, как аппаратные, так и программные, для обеспечения безопасности информации. Рассматриваемые вопросы: аппаратные средства защиты, криптографические модули, программные средства защиты, их настройка и использование.

Практическая работа №2. Организация безопасного обмена трафиком в сети. Цель: изучить методы защиты и безопасного обмена трафиком в компьютерных сетях. Задание: реализовать безопасный обмен трафиком с использованием протоколов безопасности, таких как VPN и SSL/TLS. Рассматриваемые вопросы: протоколы безопасности, методы защиты трафика, настройка VPN и SSL/TLS для защиты данных.

Практическая работа №3. Защита беспроводных сетей Wi-Fi. Цель: изучить методы защиты беспроводных сетей Wi-Fi от несанкционированного доступа и атак. Задание: настроить безопасную беспроводную сеть с использованием современных методов защиты, таких как WPA3 и шифрование трафика. Рассматриваемые вопросы: протоколы безопасности Wi-Fi, защита от атак на беспроводные сети, настройка безопасных соединений.

Практическая работа №4. Настройка и использование ACL-списков для контроля доступа в сети. Цель: изучить принципы настройки и применения списков управления доступом (ACL) для контроля доступа в компьютерной сети. Задание: настроить ACL-списки для ограничения доступа к сетевым ресурсам и протестировать их работу. Рассматриваемые вопросы: настройка и управление доступом через ACL, фильтрация трафика, безопасность и контроль доступа в сети.

7.1.2. Типовые задания для лабораторных работ

Лабораторная работа №1. Оценка устойчивости паролей и алгоритмов шифрования. Цель: изучить методы защиты паролей и алгоритмы шифрования данных для повышения безопасности информации в компьютерных системах. Задание: провести тестирование паролей на их стойкость, применить различные алгоритмы шифрования для защиты данных и оценить их эффективность. Рассматриваемые вопросы: угрозы безопасности паролей, методы защиты паролей, алгоритмы шифрования и их эффективность.

Лабораторная работа №2. Исследование методов шифрования: шифры замены и перестановки. Цель: изучить основные методы шифрования, такие как шифры замены и перестановки, и их применение для защиты информации. Задание: реализовать шифры замены и перестановки, провести их анализ с точки зрения безопасности и оценить уязвимости этих методов. Рассматриваемые вопросы: принципы работы с шифрами замены и перестановки, их сильные и слабые стороны, анализ уязвимостей.

Лабораторная работа №3. Проверка целостности данных с использованием хеш-функций. Цель: изучить методы обеспечения целостности данных с использованием хеш-функций и цифровых подписей. Задание: применить хеш-функции для проверки целостности файлов и оценить их устойчивость к изменениям. Рассматриваемые вопросы: хеш-функции, цифровые подписи, методы защиты от изменений данных.

Лабораторная работа №4. Применение шифрования для защиты файлов. Цель: изучить методы шифрования файлов для защиты конфиденциальной информации при хранении и передаче. Задание: реализовать алгоритмы шифрования для защиты файлов и оценить их эффективность с точки зрения безопасности. Рассматриваемые вопросы: методы шифрования файлов, защита данных при передаче и хранении, оценка эффективности алгоритмов шифрования.

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 междисциплинарному курсу: дифференцированный зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения профессиональных компетенций и их частей.

Вопросы для подготовки к промежуточной аттестации (дифференцированный зачет)

ПК 3.1 Осуществлять проектирование сетевой инфраструктуры

1. Какие этапы проектирования сетевой инфраструктуры необходимы для обеспечения её безопасности?
2. Как выбрать подходящие протоколы для безопасной передачи данных при проектировании сети?
3. Каковы основные принципы сегментации сети и как они влияют на безопасность инфраструктуры?
4. Что такое модель "Zero Trust" и как она применяется при проектировании безопасной сетевой инфраструктуры?
5. Как выбрать и настроить устройства для защиты периметра сети (например, фаерволы, IDS/IPS)?
6. Какова роль шифрования при проектировании безопасной сети и какие алгоритмы шифрования предпочтительны для разных типов трафика?
7. Какие способы аутентификации пользователей и устройств наиболее эффективны при проектировании защищённых сетевых решений?
8. Какие факторы необходимо учитывать при выборе и настройке VPN-сервисов для защиты удалённых пользователей и филиалов?
9. Как обеспечить отказоустойчивость и высокую доступность сетевой инфраструктуры без ущерба для безопасности?
10. Как проектировать защиту от DDoS-атак на уровне сетевой инфраструктуры?
11. Какие риски безопасности следует учитывать при проектировании сетевых соединений между локальными сетями и облачными сервисами?
12. Какую роль играют ACL (списки управления доступом) в проектировании сетевой безопасности и как их правильно настроить?
13. Как учесть безопасность IoT-устройств при проектировании корпоративной сети?
14. Какие методы защиты от несанкционированного доступа к сети следует применять в процессе проектирования беспроводных сетей?
15. Как мониторинг и анализ трафика помогают в проектировании безопасной сетевой инфраструктуры, и какие инструменты для этого используются?

ПК 3.3 Осуществлять защиту информации в сети с использованием программно-аппаратных средств

16. Какие программно-аппаратные средства используются для защиты информации в сети на уровне периметра?
17. Какую роль в защите информации в сети играют фаерволы, и как они должны быть настроены для обеспечения максимальной безопасности?
18. Что такое IDS/IPS системы и как они помогают в защите информации в сети?
19. Какую роль в защите данных в сети играет шифрование и какие алгоритмы шифрования предпочтительны для различных типов трафика?
20. Какие методы аутентификации и авторизации пользователей следует применять для повышения безопасности сети?

21. Как защитить сетевые соединения от атак с использованием технологий виртуальных частных сетей (VPN)?
22. Какие программно-аппаратные решения необходимы для защиты от атак "человек посередине" (Man-in-the-Middle)?
23. Как эффективно использовать анти-DDoS устройства и системы для защиты сетевой инфраструктуры от распределённых атак отказа в обслуживании?
24. Какие средства мониторинга и анализа трафика можно использовать для обнаружения вторжений и предотвращения угроз безопасности в сети?
25. Как защитить беспроводные сети с использованием программно-аппаратных решений, таких как WPA3, и какие угрозы необходимо учитывать?
26. Какие роли в защите информации в сети играют технологии управления доступом (например, ACL, VLAN)?
27. Какова роль хеш-функций и цифровых подписей в обеспечении целостности данных и предотвращении их подделки?
28. Какие решения для защиты конечных устройств (антивирусы, EDR) следует использовать для защиты информации на рабочих станциях и серверах?
29. Как настроить и использовать средства защиты для предотвращения утечек данных (DLP-системы) в сети?
30. Какие аппаратные устройства защиты, такие как криптографические модули (HSM), используются для защиты ключей шифрования и других критичных данных?

ПК 3.5 Модернизировать сетевые устройства информационно-коммуникационных систем

31. Какие факторы следует учитывать при модернизации сетевых устройств для повышения уровня безопасности информационно-коммуникационных систем?
32. Как правильно выбрать и настроить новые фаерволы при модернизации сетевых устройств для защиты от современных угроз?
33. Какие технологии могут быть использованы для модернизации маршрутизаторов и коммутаторов с целью повышения их безопасности?
34. Как модернизировать устройства управления доступом (например, NAS, SAN) для улучшения защиты данных в сети?
35. Какие программно-аппаратные решения можно интегрировать в процесс модернизации сетевых устройств для защиты от DDoS-атак?
36. Как улучшить защиту сети при модернизации беспроводных точек доступа с использованием современных стандартов безопасности (WPA3)?
37. Как интеграция средств мониторинга и анализа в процесс модернизации сетевых устройств помогает повысить уровень безопасности сети?
38. Какие новые криптографические протоколы следует внедрить при модернизации сетевых устройств для улучшения шифрования данных в передаче?
39. Каковы особенности модернизации средств защиты от вторжений (IDS/IPS) в сети с учетом новых угроз?
40. Какие методы защиты можно добавить при модернизации межсетевых экранов для более эффективной фильтрации трафика и предотвращения несанкционированного доступа?
41. Как модернизация серверов и рабочих станций может повлиять на безопасность сети и какие меры следует предпринять для защиты этих устройств?
42. Какие аппаратные средства, такие как криптографические модули (HSM), должны быть интегрированы в процессе модернизации для улучшения защиты данных?
43. Как выбрать и настроить более защищённые решения для виртуализации сетевых устройств при модернизации сетевой инфраструктуры?
44. Как модернизация сетевых устройств помогает обеспечить отказоустойчивость и высокую доступность при атакующих угрозах?

45. Какие средства защиты от утечек данных (DLP-системы) следует интегрировать при модернизации сетевых устройств для обеспечения контроля за передаваемой информацией?