СОЧИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)
федерального государственного автономного образовательного
учреждения высшего образования
«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ»

Отделение среднего профессионального образования

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

"Безопасность функционирования информационных систем"

(наименование дисциплины)

Освоение учебной дисциплины ведется в рамках реализации основной образовательной программы среднего профессионального образования (ОП СПО):

09.02.06 Сетевое и системное администрирование

(код и наименование специальности/профессии ОП СПО)

Квалификация:

сетевой и системный администратор

(наименование квалификации)

Сочи,
2023 г.

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ПМ.03.02 Безопасность функционирования информационных систем

название дисциплины

1.1. Область применения программы

Программа учебной дисциплины ПМ.03.02 Безопасность функционирования информационных систем является частью программы подготовки специалистов среднего звена в соответствии с ФГОС "Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование (приказ Минобрнауки России от 09.12.2016 г. № 1548)"

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена.

Учебная дисциплина ПМ.03.02 Безопасность функционирования информационных систем входит в Профессиональный цикл Профессиональной подготовки.

1.3. Цели и задачи – требования к результатам освоения учебной дисциплины.

Способствовать формированию общих и профессиональных компетенций посредством приобретения знаний, умений и навыков в соответствии с видом профессиональной деятельности.

В результате освоения учебной дисциплины студент должен знать:

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

В результате освоения учебной дисциплины студент должен 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.

В результате освоения учебной дисциплины студент должен иметь навыки и (или) опыт деятельности:

- обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя;
- удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры;
- поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры.

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Объем программы 144 часов, в том числе:
аудиторной учебной нагрузки обучающегося 120 часов;
самостоятельной работы обучающегося 24 часов.

2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
2.1. Объем учебной дисциплины и виды учебной работы

Таблица 1. Виды учебной работы по периодам освоения ООП СПО для формы обучения - очная.

Вид учебной работы	Всего, ак. ч.	Семестр(-ы)					
		7	8				
Контактная (аудиторная) работа (всего)	120	30	90				
в том числе:	-	-	-	-	-	-	-
лекции (если предусмотрено)	48	12	36				
в том числе в форме практической подготовки (если предусмотрено)	-	-	-				
лабораторные занятия (если предусмотрено)	-	-	-				
в том числе в форме практической подготовки (если предусмотрено)	-	-	-				
практические занятия (если предусмотрено)	72	18	54				
в том числе в форме практической подготовки (если предусмотрено)	24	6	18				
Самостоятельная работа обучающегося (всего)	24	6	18				
в том числе:	-	-	-	-	-	-	-
в форме практической подготовки (если предусмотрено)	-	-	-				
Часов на контроль:	-	-	-				
Промежуточная аттестация в форме: (зачет/дифзачет/ экзамен)	-	ЗаО	ЗаО				
Общая трудоемкость час	144	36	108				

2.2. Тематический план и содержание учебной дисциплины ПМ.03.02 Безопасность функционирования информационных систем

Таблица 2. Содержание дисциплины/МДК по видам учебной работы

НАИМЕНОВАНИЕ РАЗДЕЛА ДИСЦИПЛИНЫ Содержание раздела (темы)	Вид учебной работы*	Кол-во часов
Основы информационной безопасности	**34**	
Понятие национальной безопасности.	Лек	2
Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.		
Информационная безопасность в системе национальной безопасности Российской Федерации.	Лек	2
Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере.		
Государственная информационная политика.	Лек	2
Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.		
Проблемы информационной войны.	Лек	2
Информационное оружие и его классификация. Информационная война.		
Информационные системы.	Лек	2
Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах.		

Методы и модели оценки уязвимости информации.	Лек	2
Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита»		
Программирование арифметических алгоритмов	Пр	4
Цели и задачи криптографии. Исследование и разработка основных методов симметричных криптосистем.		
Программирование арифметических алгоритмов	Пр	4
Шифрование методом замены. Шифр Цезаря.		
Определение объектов защиты на типовом объекте информатизации.	Пр	8
Классификация защищаемой информации по видам тайны и степеням конфиденциальности.		
Систематическая проработка конспектов занятий.	СР	6
Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).		
Проблемы информационной безопасности.	**16**	
Основные понятия и анализ угроз информационной безопасности.	Лек	2
Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.		
Проблемы информационной безопасности сетей.	Лек	6
Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей.		
Политика безопасности.	Лек	4
Основные понятия политики безопасности. Структура политики безопасности организации.		
Стандарты информационной безопасности.	Лек	2
Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий		
Определение угроз объекта информатизации.	Пр	2
Определение угроз объекта информатизации и их классификация.		
Технологии защиты данных.	**18**	
Принципы криптографической защиты информации.	Лек	2
Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования. Электронная цифровая подпись и функция хэширования.		
Криптографические алгоритмы.	Лек	2
Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы.		
Технологии аутентификации.	Лек	2
Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.		
Криптографическое шифрование методом простой замены.	Пр	6
Криптографическое шифрование методом многоалфавитной одноконтурной замены.		
Криптографическое шифрование	Пр	4
Криптографическое шифрование методом усложнённой перестановки по маршрутам.		
Хэш-функции и цифровая подпись.	Пр	2
Изучение отечественных стандартов хэш-функции и цифровой подписи.		

Технологии защиты межсетевого обмена данными.	**43**	
Обеспечение безопасности операционных систем.	Лек	2
Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС.		
Технологии межсетевых экранов.	Лек	2
Функции межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ.		
Основы технологии виртуальных защищенных сетей VPN.	Лек	2
Концепция построения виртуальных защищенных сетей VPN. VPN-решения для построения защищенных сетей. Достоинства применения технологий VPN		
Защита на канальном и сеансовом уровнях.	Лек	2
Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне. Защита беспроводных сетей.		
Защита на сетевом уровне - протокол IPSEC.	Лек	2
Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол управления криптоключами I KE . Особенности реализации средств IPSec.		
Инфраструктура защиты на прикладном уровне.	Лек	2
Управление идентификацией и доступом. Организация защищенного удаленного доступа. Управление доступом по схеме однократного входа с авторизацией Single Sign-On. Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.		
Компоненты межсетевого экрана.	Пр	2
Политика межсетевого экранирования.		
Задачи, решаемые VPN.	Пр	4
Задачи, решаемые VPN. Уровни защищенных каналов.		
Организация VPN средствами СЗИ VipNet.	Пр	4
Использование протокола IPSec для защиты сетей.		
Создание ключей PGP.	Пр	4
Создание ключей PGP. Передача открытого ключа PGP корреспондентам.		
Настройка системы предотвращения вторжений (IPS)	Пр	4
Настройка безопасности на втором уровне на коммутаторах	Пр	4
Подготовка к лабораторно-практическим работам	СР	9
Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите.		
Технологии обнаружения вторжений.	**33**	
Анализ защищенности и обнаружение атак.	Лек	2
Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак.		
Защита от вирусов. Методы управления средствами сетевой безопасности.	Лек	2
Компьютерные вирусы и проблемы антивирусной защиты. Антивирусные программы и комплексы. Построение системы антивирусной защиты корпоративной сети. Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности		
Сигнатурный анализ и обнаружение аномалий	Пр	2
Обнаружение в реальном времени и отложенный анализ	Пр	4
Обнаружение в реальном времени и отложенный анализ. Локальные и сетевые системы обнаружения атак.		
Распределенные системы обнаружения атак.	Пр	4
Распределенные системы обнаружения атак. Система обнаружения атак Snort.		
Базовая настройка шлюза безопасности ASA.	Пр	4
Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки		

Настройка Site-to-SiteVPN.	Пр	6
Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.		
Подготовка к лабораторно-практическим работам	СР	9
Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите.		

** - Лек – лекции; Пр – практические занятия; СР – самостоятельная работа; ЛР – лабораторные работы.*

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы учебной дисциплины предусмотрены специальные помещения, приведенным в п 6.3 основной образовательной программы специальности.

Таблица 3. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории Специализированное учебное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Учебная аудитория для проведения занятий лекционного типа, практических занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Комплект специализированной мебели, маркерная доска; кафедра; автоматизированное рабочее место преподавателя: компьютер AMD Ryzen, монитор LCD 24" Philips, интерактивная панель 86", имеется выход в интернет Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный
Учебная аудитория для проведения занятий лекционного типа, практических занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (Компьютерный класс)	Комплект специализированной мебели; доска аудиторная меловая, автоматизированные рабочие места (процессор не ниже Intel Core i5, оперативная память объемом не менее 16Gb;(SSD 500 GB HDD 1 TB); проектор EPSON, проекционный экран, имеется выход в интернет Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный
Аудитория для самостоятельной работы обучающихся	Комплект специализированной мебели; Телевизор LED LG 42" автоматизированные рабочие места (процессор не ниже AMD Ryzen, оперативная память объемом не менее 8 Гб; SDD 500 GB, моноблок Lenovo Intel i3), имеется выход в интернет Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Дополнительные источники:

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров:

- Электронно-библиотечная система РУДН – ЭБС РУДН http://mega.rudn.ru/MegaPro/Web
- Образовательная платформа Юрайт https://urait.ru
- ЭБС Znanium https://znanium.ru
- научная электронная библиотека eLIBRARY.RU https://www.elibrary.ru/
- ЭБС «Academia-library» https://academia-moscow.ru/

2. Базы данных и поисковые системы:

- Учебный портал института https://portal.rudn-sochi.ru/

Методические материалы для обучающихся

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Таблица 4. Контроль и оценка результатов освоения дисциплины

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Знания: - архитектуру и функции систем управления сетями, стандарты систем управления; - средства мониторинга и анализа локальных сетей; - методы устранения неисправностей в технических средства	Анализ и оценка выполнения индивидуальных заданий, расчетных работ, опрос, тематический диктант, контрольная работа, практические занятия, домашние работы, компьютерное тестирование, Взаимоконтроль и самоконтроль студентов. Полнота и грамотность подготовленных докладов, сообщений, презентаций.
Умения: - 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.	Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, беседа, опрос, практические занятия, домашние работы, компьютерное тестирование
Практический опыт: - обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя; - удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры; - поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры.	Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, выполнение и защита индивидуальных заданий.

5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 5. Перечень компетенций

Шифр	**Результаты (компетенции)** **Основные показатели результатов подготовки**
ПК 3.1.	**Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.**
Знать: архитектуру и функции систем управления сетями, стандарты систем управления;	
Уметь: выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств	

ПК 3.2.	**Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.**
Знать: средства мониторинга и анализа локальных сетей;	
ПК 3.3.	**Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации.**
Уметь: осуществлять диагностику и поиск неисправностей всех компонентов сети;	
ПК 3.4.	**Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.**
Владеть: поддержкой пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры	
ПК 3.5.	**Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.**
Владеть: обслуживанием сетевой инфраструктуры, восстановлении работоспособности сети после сбоя	
ПК 3.6.	**Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.**
Знать: методы устранения неисправностей в технических средствах	
Уметь: выполнять действия по устранению неисправностей	

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Безопасность функционирования информационных

Перечень вопросов для подготовки к занятиям и промежуточной аттестации, контрольных работ, содержание заданий для выполнения практических и самостоятельных работ, рекомендации по выполнению и критерии оценивания представлены в фонде оценочных средств по дисциплине «Безопасность функционирования информационных систем» в Приложении к настоящей Рабочей программе дисциплины.

Оценочные средства позволяют провести текущий контроль по дисциплине. По каждому средству оценивается полнота и глубина освоения, характеризующиеся показателями и критериями оценивания

Таблица 6. Показатели и критерии оценивания

Показатель	Критерий
Пороговый (узнавание) «3»	Знает: базовые общие знания; Умеет: основные умения, требуемые для выполнения простых задач; Владеет: работает при прямом наблюдении.
Базовый (воспроизведение) «4»	Знает: факты, принципы, процессы, общие понятия в пределах области исследования; Умеет: диапазон практических умений, требуемых для решения определенных проблем в области исследования; Владеет: берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Высокий (компетентность) «5» max балл	Знает: фактическое и теоретическое знание в пределах области исследования с пониманием границ применимости; Умеет: диапазон практических умений, требуемых для развития творческих решений, абстрагирования проблем; Владеет: контролирует работу, проводит оценку, совершенствует действия работы

Максимальное количество баллов по каждому оценочному средству соответствует вербальному критерию «высокий».

7. ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

7.1 Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

В процессе обучения используются активные и интерактивные образовательные технологии (формы проведения занятий):

-лекции, фронтальные опросы, презентации и защита мини-проектов;

-кейс-стади (разбор конкретных ситуаций),

-имитационные компьютерные модели;

-организации самостоятельной учебно-познавательной деятельности (индивидуальные домашние задания).