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

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,
2021 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)"

Цель изучения МДК.03.02 «Безопасность функционирования информационных систем» – является формирование знаний об объектах и задачах защиты компьютерных систем, способах и средствах нарушения информационной безопасности, о принципах и подходах к
решению задач защиты информации; а также формирование умений по применению современных технологий, выбора средств и инструментов защиты информации для построения современных защищенных информационных систем.

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.

- изучение основ проектирования и эксплуатации защищенных информационных систем;
- изучение принципов администрирования сетевых служб;
- изучение способов обеспечения работоспособности и доступности серверов;
- изучение клиентской части программного обеспечения.

В результате освоения учебной дисциплины студент должен знать:

В результате освоения учебной дисциплины студент должен уметь:

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

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)					
		8	2				
Контактная (аудиторная) работа (всего)	120	120	34				
в том числе:	-	-	-	-	-	-	-
лекции (если предусмотрено)	48	48	-				
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	72	34				
в том числе в форме практической подготовки (если предусмотрено)	24	24	-				
Самостоятельная работа обучающегося (всего)	24	24	4				
в том числе:	-	-	-	-	-	-	-
в форме практической подготовки (если предусмотрено)	-	-	-				
Часов на контроль:	-	-	18				
Промежуточная аттестация в форме: (зачет/дифзачет/ экзамен)	-	ЗаО	Эк				
Общая трудоемкость час	144	144	56				

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 проектирования и эксплуатации защищенных информационных систем	**20**	
Основные понятия и определения.	Лек	2
Понятие информации, информационного ресурса, информационной системы. Критичность информационного ресурса. Основные особенности информационной системы. Разработка концептуального плана защиты. Принципы проектирования защиты информации. Рекомендации по проектированию защищенных элементов ИС. Укрепление защиты внутренней		
Работа с конспектом.	СР	2
Составить конспект на тему «Основные особенности информационной системы»		
Проблема обеспечения безопасности в информационных системах.	Лек	2
Основные причины реализации угроз информационной безопасности. Классификация угроз по используемым средствам. Классификация по характеру действий, используемых в атаке. Классификация по характеру уязвимостей. Классификация типовых удаленных атак по виду воздействия.		
Работа с конспектом.	СР	2
Составить конспект на тему «Классификация угроз по используемым средствам»		
Специфика эксплуатации защищенных ИС.	Лек	2
Основная особенность эксплуатации средств и систем информационной безопасности. Возрастание сложности ИС, новые угрозы безопасности, особенности ИС.		

Работа с конспектом.	СР	2
Составить конспект на тему «Основная особенность эксплуатации средств и систем информационной безопасности»		
Концепция проектирования системы защиты ИС.	Лек	2
Анализ бизнес-требований к защите информации в ИС, влияние общих бизнес-факторов на проект защиты. Снижение влияния несовместимости систем на их защиту. Угрозы безопасности ИС, возникающие из-за проблем с сопровождением.		
Общий состав работ на этапе эксплуатации IT-систем.	Лек	2
Понятие грамотной эксплуатации системы. Мониторинг в режиме реального времени и анализ происходящих в ИС событий. Контроль безопасности системы. Преодоление нештатных ситуаций. Техническая поддержка средств и систем защиты. Анализ и контроль защищенности ресурсов.		
Требования по защите информационных систем.	Лек	2
Требования по защите информации от НСД в соответствии с Руководящими Документами России. Понятие класса защищенности, групп автоматизированных систем. Требования к подсистемам защиты для каждого класса защищенности. Основные меры защиты информации в автоматизированных системах. Основные положения и требования для обеспечения защиты информации в процессе эксплуатации.		
Работа с конспектом.	СР	2
Составить конспект на тему «Основные меры защиты информации в автоматизированных системах информационной безопасности»		
Внедрение, конфигурирование и обеспечение безопасности службы каталога Active Directory для Windows Server.	**24**	
Обзор службы каталога Active Directory Windows Server	Лек	2
Основные понятия. Домен. Контроллеры домена. Дерево. Лес.		
Логическая структура службы Active Directory	Лек	2
Основные функции контроллеров домена. Контроллеры домена специального назначения. Серверы глобального каталога. Структурные объекты БД Active Directory. Разделы Active Directory. Домены. Деревья доменов. Леса. Доверительные отношения. Организационные единицы. Использование организационных единиц для управления группами объектов.		
Проектирование и реализация службы Active Directory	Лек	2
Проектирование структуры леса. Проектирование доменной структуры. Определение количества доменов. Проектирование инфраструктуры DNS. Проектирование структуры организационных единиц.		
Работа с конспектом.	СР	2
Составить конспект на тему «Проектирование инфраструктуры DNS»		
Безопасное администрирование службы Active Directory.	Лек	4
Основные методы обеспечения безопасности Active Directory. Участники безопасности. Списки управления доступом. Лексема доступа. Аутентификация и разрешение. Защита Active Directory с использованием протокола Kerberos. Управление объектами Active Directory. Использование групповых политик Active Directory.		
Конфигурирование службы каталога Active Directory	Пр	8
Цель — познакомиться на практике с особенностями практической реализации и настройки службы каталога Active Directory для Windows Server.		
Работа с конспектом.	СР	2
Составить опорный конспект на тему «Основные методы обеспечения безопасности Active Directory»		
Работа с конспектом.	СР	2
Составить опорный конспект на тему «Конфигурирование службы каталога Active Directory»		

Администрирование сетевых служб.	**58**	
Сканеры безопасности.	Лек	2
Понятия уязвимости, угрозы. Определение сканера безопасности. Принципы работы сканера безопасности. Классы сканеров безопасности и их краткая характеристика. Недостатки сканеров безопасности.		
Подготовка к лабораторной работе.	СР	2
Подготовка к лабораторной работе «Сканеры безопасности сетевых сервисов и протоколов»		
Сканеры безопасности сетевых сервисов и протоколов	Пр	8
Цель — познакомиться на практике с проблемой обнаружения уязвимостей сетевого узла при помощи сканеров безопасности. Определить способы устранения обнаруженных уязвимостей.		
Подготовка к лабораторной работе	СР	2
Подготовка к лабораторной работе «Сканеры безопасности операционных систем»		
Сканеры безопасности операционных систем	Пр	8
Цель — познакомиться на практике со сканером безопасности уровня ОС System Scanner. Выявить отличия между сканерами безопасности локальных и удаленных систем.		
Межсетевые экраны.	Лек	2
Риски, связанные с подключением компьютера к глобальной сети Интернет, понятие межсетевого экрана. Виды межсетевых экранов и их кратная характеристика, правила функционирования межсетевых экранов.		
Подготовка к лабораторной работе	СР	2
Подготовка к лабораторной работе «Межсетевые экраны и фильтры»		
Межсетевые экраны и фильтры.	Пр	8
Цель — познакомиться на практике с особенностями конфигурирования межсетевых экранов и фильтров на примере программ Outpost Firewall Pro и Kerio WinRoute Firewall.		
Виртуальные частные сети.	Лек	2
Понятие виртуальных частных сетей, криптозащищенных туннелей, инициатора и терминатора туннеля. Протоколы поддержки виртуальных частных сетей.		
Построение VPN	Пр	8
Цель — познакомиться на практике с организацией виртуальных частных сетей средствами Windows Server		
Системы обнаружения вторжений.	Лек	2
Понятие системы обнаружения вторжений. Основные виды систем обнаружения вторжений. Достоинства и недостатки. Понятие сниффинга. Снифферы, их легальное и нелегальное применение.		
Лабораторная работа.	Пр	8
Цель — познакомиться на практике с методами и средствами обнаружения вторжений.		
Защита беспроводных сетей.	Лек	2
Стандарты и топологии беспроводных сетей. Понятие точки доступа. Защита беспроводных сетей, основные угрозы безопасности беспроводных сетей. Управление беспроводными сетями при помощи групповых политик. Шифрование трафика беспроводной сети. Методы аутентификации пользователей в беспроводных сетях.		
Выбор средств защиты для границ ИС.	Лек	2
Рекомендации по межсетевым экранам. Понятие демилитаризированной зоны. Рекомендации по прокси-серверам. Рекомендации по IDS. Рекомендации по VPN. Практическое использование средств защиты для границ ИС.		
Безопасное администрирование сетевых служб в LINUX	**24**	
Средства для фильтрации сетевых пакетов: iptables и ipchains.	Лек	4
Краткое введение в фильтрацию пакетов. Таблица Mangle. Таблица NAT. Таблица Filter. Движение пакетов. Построение правил.		

Безопасность сетевой файловой системы nfs.	Лек	2
Понятие сетевой файловой системы nfs. Безопасность nfs: основная проблема nfs и способы обеспечения безопасности.		
Безопасность ftp,web-сервера apache.	Лек	2
Протокол ftp, понятие анонимного доступа к ftp-серверу. способы взлома и защита от них. Назначение и базовая конфигурация apache. конфигурирование apache.		
Установка и настройка FTP-севера proftpd	Пр	8
Цель — Познакомиться на практике с FTP-сервером Proftpd		
Установка и настройка WEB-севера Apache	Пр	8
Цель — Познакомиться на практике с системой управления пакетов ОС Debian и базовой настройкой WEB-сервера Apache.		
Внедрение инфраструктуры открытых ключей	**12**	
Развертывание инфраструктуры открытых ключей	Лек	2
Проектирование PKI — Формирование политики PKI. Модель доверия и архитектура PKI. Политика применения сертификатов. Выбор программного продукта или поставщика услуг PKI. Интеграция PKI с действующими системами и приложениями. Серверы и криптографическое аппаратное обеспечение. Смарт-карты и считыватели. Физическая среда. Управление и администрирование системы PKI. Внедрение PKI — Создание прототипа. Пилотный проект. Внедрение.		
Подготовка к лабораторной работе	СР	2
Подготовка к лабораторной работе «Развертывание PKI на базе «КриптоПро УЦ»»		
Развертывание PKI на базе «КриптоПро УЦ	Пр	4
Цель — изучить принципы построения инфраструктуры открытых ключей. Научиться устанавливать и конфигурировать ПАК «КриптоПро УЦ».		
Подготовка к лабораторной работе	СР	2
Подготовка к лабораторной работе «Регистрация пользователей, изготовление и управление сертификатами в «КриптоПро УЦ»		
Регистрация пользователей, изготовление и управление сертификатами в «КриптоПро УЦ	Пр	2
Цель — познакомиться на практике с процедурой регистрации пользователей удостоверяющего центра и управлением жизненным циклом сертификатов их открытых ключей.		
Обеспечение работоспособности и доступности серверов	**6**	
Организация резервного копирования на серверах Windows.	Лек	2
Оборудование для архивации. Типы архивации. Создание плана резервного копирования и выбор архивируемых данных.		
RAID и зеркалирование.	Лек	2
Классификация RAID-массивов. Комбинированные уровни RAID. Программный RAID в Windows и Linux		
Программный RAID в ОС Windows	Пр	2
Цель — Познакомиться на практике с методами обеспечения надежного хранения данных и организацией программного RAID-массива в Windows.		

** - 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

Основные источники:

1. Кияев В., Граничин О. Безопасность информационных систем: курс : учебное пособие. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. - Текст : электронный. - URL: https://biblioclub.ru/index.php?page=book&id=429032
2. Васильков А.В., Васильков И. А. Безопасность и управление доступом в информационных системах : Учебное пособие. - Москва: Издательство "ФОРУМ", 2022. - 368 с. - Текст : электронный. - URL: https://znanium.com/catalog/document?id=399436

Дополнительные источники:

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:	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:	Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, беседа, опрос, практические занятия, домашние работы, компьютерное тестирование
Практический опыт:	Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, выполнение и защита индивидуальных заданий.

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).