АННОТАЦИЯ

Рабочая программа учебной дисциплины
МДК.03.02 БЕЗОПАСНОСТЬ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

специальность 09.02.02 Компьютерные сети

ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Область применения программы

Рабочая программа учебной дисциплины «Безопасность функционирования информационных систем» является частью основной профессиональной образовательной программы в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее ФГОС СПО) для специальности 09.02.02 Компьютерные сети.

1.2 Место дисциплины в структуре программы подготовки специалистов среднего звена

Дисциплина «Безопасность функционирования информационных систем» относится к профессиональному модулю «Эксплуатация объектов сетевой инфраструктуры».

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

В результате изучения профессионального модуля обучающийся должен *иметь практический опыт:*

- обслуживания сетевой инфраструктуры;
- удаленного администрирования сетевой инфраструктуры;
- поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры.

В результате освоения дисциплины обучающийся должен *уметь*:

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- правильно оформлять техническую документацию;
- наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;
- устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту.

В результате освоения дисциплины обучающийся должен *знать*:

- задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;
- средства мониторинга и анализа локальных сетей;
- основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;
- основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Максимальная учебная нагрузка обучающегося 195 часов, в том числе:
обязательная аудиторная учебная нагрузка обучающегося 130 часов;

самостоятельная работа обучающегося 65 часов.

1.5. Перечень планируемых результатов обучения по дисциплине (Перечень формируемых компетенций)

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

1.6. Тематический план и содержание учебной дисциплины МДК.03.02 Безопасность функционирования информационных систем

Наименование разделов и тем	**Содержание учебного материала, практические и лабораторные работы, самостоятельная работа обучающихся**	**Объем часов**
1	**2**	**3**
Раздел 1.	***Содержание учебного материала***	**44**

Наименование разделов и тем	Содержание учебного материала, практические и лабораторные работы, самостоятельная работа обучающихся	Объем часов
Основы информационной безопасности	***Лекции*** Понятие национальной безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации Государственная информационная политика Информация - наиболее ценный ресурс современного общества Проблемы информационной войны Проблемы информационной безопасности в сфере государственного и муниципального управления Информационные системы Методы и модели оценки уязвимости информации	20
	Практические занятия Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права Подготовка описания охраняемой информации, модели угроз, построение модели информационной безопасности	8
	Самостоятельная работа Работа с конспектом. Выполнение заданий практической работы. Подготовка рефератов	16
Раздел 2. Проблемы информационной безопасности	***Содержание учебного материала***	**42**
	Лекции Основные понятия и анализ угроз информационной безопасности. Проблемы информационной безопасности сетей. Политика безопасности. Стандарты информационной безопасности.	10
	Практические занятия Проведение анализа сравнительных характеристик у каналов утечки информации Исследование проблем создания и развития национальной системы управления цифровыми сертификатами Исследование защиты в среде Windows , Linux	12
	Лабораторные занятия Использование встроенных средств ОС для обеспечения безопасности Установка программных средств защиты (программные прокси-серверы, диагностические программы и т.п.)	4
	Самостоятельная работа Работа с конспектом. Выполнение заданий практической работы. Подготовка рефератов	16
Раздел 3. Технологии защиты данных	***Содержание учебного материала***	**46**
	Лекции Принципы криптографической защиты информации. Криптографические алгоритмы. Технологии аутентификации.	8

Наименование разделов и тем	Содержание учебного материала, практические и лабораторные работы, самостоятельная работа обучающихся	Объем часов
	Практические занятия Составление описания основных классов вирусов Системы обнаружения вторжений Количественная оценка стойкости парольной защиты. Описание механизмов и принципов работы систем шифрования с открытым ключом. Изучение стандарта криптографической защиты AES (Advanced Encryption Standart). Изучение отечественных стандартов хэш-функции и цифровой подписи.	18
	Лабораторные занятия Управление пользователями и их правами доступа в ОС Использование программы Ethereal для анализа сетевого трафика	4
	Самостоятельная работа Работа с конспектом. Выполнение заданий практической работы. Подготовка рефератов	16
Раздел 4. Технологии защиты межсетевого обмена данными	***Содержание учебного материала***	**63**
	Лекции Обеспечение безопасности операционных систем. Технологии межсетевых экранов. Основы технологии виртуальных защищенных сетей VPN. Защита на канальном и сеансовом уровнях. Защита на сетевом уровне - протокол IPSEC. Инфраструктура защиты на прикладном уровне. Анализ защищенности и обнаружение атак. Защита от вирусов. Методы управления средствами сетевой безопасности. Построение системы антивирусной защиты корпоративной сети.	22
	Практические занятия Сканеры безопасности операционных систем. Сканеры безопасности сетевых сервисов и протоколов Межсетевые экраны и фильтры: Outpost Firewall Pro Компоненты межсетевого экрана. Политика межсетевого экранирования. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне. Организация VPN средствами СЗИ VipNet. Использование протокола IPSec для защиты сетей. Защита на транспортном уровне. Организация VPN средствами протокола SSL в Windows Server. Распределенные системы обнаружения атак. Система обнаружения атак Snort.	22
	Лабораторные работы Анализ протоколов Ethernet ARP, TCP, IP	2

Наименование разделов и тем	Содержание учебного материала, практические и лабораторные работы, самостоятельная работа обучающихся	Объем часов
	Самостоятельная работа Работа с конспектом. Выполнение заданий практической работы. Подготовка рефератов	17
Всего:		

1.7. Вид промежуточного контроля: дифференцированный зачет

1.8. Основная литература

1. Кияев, В. Безопасность информационных систем : курс / В. Кияев, О. Граничин. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с. : ил. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429032
2. Заика, А. Компьютерная безопасность / А. Заика. - М. : Рипол Классик, 2013. - 160 с. - (Компьютер — это просто). - ISBN 978-5-386-06476-1 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=227317
3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. [Электронный ресурс] : Учебные пособия — Электрон. дан. — М. : Горячая линия-Телеком, 2013. — 338 с. — Режим доступа: http://e.lanbook.com/book/63235
4. Лапонина, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=429094

Составитель: канд. тех. наук, доцент С.А. Осипов