ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А.БУНИНА

«УТВЕРЖДАЮ»
Директор института СПО
/ М.А. Харламова

РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ

МДК.03.02 Безопасность функционирования информационных систем

09.02.02 Компьютерные сети

Базовый уровень подготовки

Форма обучения: **очная**

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.02 Компьютерные сети, утвержденного приказом Министерства образования и науки Российской Федерации от «28» июля 2014 г. № 803

Место дисциплины в структуре ППССЗ СПО МДК.03.02 Безопасность функционирования информационных систем

Учебная дисциплина МДК.03.02 Безопасность функционирования информационных систем входит в состав профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры

Рабочая программа разработана на кафедре математического моделирования, компьютерных технологий и информационной безопасности

Зав. кафедрой: О.Н. Масина

Разработчик(и) рабочей программы:

Преподаватель института СПО Лаухин В.В.

Рецензент

доцент, к. п. н., Щучка Т.А.

СОДЕРЖАНИЕ

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

1.1. Область применения программы
Рабочая программа учебной дисциплины является частью образовательной программы в соответствии с ФГОС по специальности 09.02.02 Компьютерные сети.
Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке по смежным специальностям.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:
Шифр дисциплины по учебному плану: МДК.03.02.
Дисциплина является частью профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры учебного плана по специальности СПО 09.02.02 – Компьютерные сети. Направлена на формирование следующих общих и профессиональных компетенций: ОК1, ОК2, ОК3, ОК4, ОК5, ОК6, ОК7, ОК8, ОК9, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6.

1.3. Цели и задачи дисциплины – требования к результатам освоения содержания дисциплины
С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения МДК.03.02 должен:

уметь:
- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры;
- осуществлять диагностику и поиск неисправностей технических средств;
- выполнять действия по устранению неисправностей в части, касающейся полномочий техника;
- тестировать кабели и коммуникационные устройства;
- выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;
- 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;

знать:
- архитектуру и функции систем управления сетями, стандарты систем управления;
- задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;
- средства мониторинга и анализа локальных сетей;
- классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;

- правила эксплуатации технических средств сетевой инфраструктуры;
- расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;
- методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;
- 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.

иметь практический опыт:
- обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;
- удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;
- организации бесперебойной работы системы по резервному копированию и восстановлению информации;
- поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры.

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС СПО и ОПОП СПО по данной специальности:

а) общих (ОК):

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 решения 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 в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

б) профессиональных (ПК):

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 схем 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.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:
максимальной учебной нагрузки обучающегося 260 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 175 часов;
самостоятельной работы обучающегося 81 час.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**260**
Обязательная аудиторная учебная нагрузка (всего)	**175**
в том числе:	
лекционные занятия	**65**
лабораторные занятия	**-**
практические занятия	**90**
контрольные работы	**-**
курсовая работа (проект) (если предусмотрено)	**20**
консультация	**4**
Самостоятельная работа обучающегося (всего)	**81**
в том числе:	
реферат	**13**
домашняя работа	**13**
Промежуточная аттестация в форме: экзамен в 8 семестре	

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

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	2		4	5
МДК 03.02. Безопасность функционирования информационных систем			**260**	
Раздел 6. Защита деятельности информационных систем				
Тема 6.1 Основы информационной безопасности	**Содержание**		**48**	
	1	**Понятие национальной безопасности.** Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.	**2**	**2, 3**
	2	**Информационная безопасность в системе национальной безопасности Российской Федерации.** Основные понятия, общеметодологические принципы обеспечения информационной безопасности. Национальные интересы в информационной сфере. Источники и содержание угроз в информационной сфере.	**4**	**2, 3**
	3	**Государственная информационная политика.** Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.	**4**	**1, 2, 3**
	4	**Информация - наиболее ценный ресурс современного общества.** Понятие «информационный ресурс». Классы информационных ресурсов.	**2**	**2, 3**
	5	**Проблемы информационной войны.** Информационное оружие и его классификация. Информационная война.	**2**	**2, 3**
	6	**Проблемы информационной безопасности в сфере государственного и муниципального управления.**	**4**	**2, 3**

		Информационные процессы в сфере государственного и муниципального управления. Виды информации и информационных ресурсов в сфере ГМУ. Состояние и перспективы информатизации сферы ГМУ.		
	7	**Информационные системы.** Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах.	**4**	**2, 3**
	8	**Методы и модели оценки уязвимости информации.** Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита»	**2**	**2, 3**
	Практические занятия			
	1.	Установка программы Ethereal и подготовка к захвату.	**4**	
	2.	Пользовательский интерфейс программы Ethereal. Фильтр отображения пакетов. Поиск кадров.	**4**	**2, 3**
	3.	Выделение ключевых кадров. Сохранение данных захвата. Печать информации. Просмотр кадра в отдельном окне.	**4**	**2, 3**
	4.	Анализ протоколов Ethernet и ARP.	**4**	**2, 3**
	5.	Анализ протоколов IP и ICMP.	**4**	**2, 3**
	6.	Анализ протокола TCP	**4**	**2, 3**
Тема 6.2. Проблемы информационной безопасности	**Содержание**		**56**	
	1	**Основные понятия и анализ угроз информационной безопасности.** Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.	**4**	**2, 3**
	2	**Проблемы информационной безопасности сетей.** Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей.	**4**	**2, 3**
	3	**Политика безопасности.** Основные понятия политики безопасности. Структура политики безопасности организации.	**2**	**2, 3**
	4	**Стандарты информационной безопасности.** Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий	**2**	**2, 3**

	Практические занятия			
	1	Система анализа рисков проверки политики информационной безопасности предприятия.	**4**	**2, 3**
	2	Этапы сетевой атаки. Исследование сетевой топологии.	**6**	**2, 3**
	3	Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы. Реализации атак. Выявление атаки на протокол SMB.	**4**	**2, 3**
	Самостоятельная работа Систематическая проработка конспектов занятий, учебной и специальной технической литературы по контрольным вопросам. Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. Подготовка индивидуального задания по теме «Стандарты информационной безопасности»		**30**	**2, 3**
Тема 6.3. Технологии защиты данных	**Содержание**		**22**	
	1	**Принципы криптографической защиты информации.** Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Комбинированная криптосистема шифрования. Электронная цифровая подпись и функция хэширования.	**4**	**2, 3**
	2	**Криптографические алгоритмы.** Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы.	**2**	**2, 3**
	3	**Технологии аутентификации.** Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.	**4**	**2, 3**
	Практические занятия			
	1	Изучение стандарта криптографической защиты AES (Advanced Encryption Standart).	**6**	**2, 3**
	2	Изучение отечественных стандартов хэш-функции и цифровой подписи	**6**	**2, 3**
	Содержание		**66**	
	1	**Обеспечение безопасности операционных систем.**	**2**	**2, 3**

Тема 6.4. Технологии защиты межсетевого обмена данными		Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС.		
	2	**Технологии межсетевых экранов.** Функции межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ.	**4**	**2, 3**
	3	**Основы технологии виртуальных защищенных сетей VPN.** Концепция построения виртуальных защищенных сетей VPN. VPN-решения для построения защищенных сетей. Достоинства применения технологий VPN.	**2**	**2, 3**
	4	**Защита на канальном и сеансовом уровнях.** Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне. Защита беспроводных сетей.	4	2, 3
	5	**Защита на сетевом уровне - протокол IPSEC.** Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP. Протокол управления криптоключами IKE. Особенности реализации средств IPSec.	2	2, 3
	Практические занятия			
	1	Компоненты межсетевого экрана. Политика межсетевого экранирования. Архитектура МЭ. Пример реализации политики МЭ.	4	2, 3
	2.	Применение МЭ на основе двудомного узла. Применение МЭ на основе фильтрующего маршрутизатора. Применение МЭ на основе экранирующего узла	4	2, 3
	3.	Применение технологии трансляции сетевых адресов. Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.	4	2, 3
	4.	Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне	4	2, 3
	5.	Организация VPN средствами СЗИ VipNet. Использование протокола IPSec для защиты сетей. Организация VPN средствами СЗИ StrongNet	4	2, 3
	6.	Организация VPN средствами протокола SSL в Windows Server	4	2, 3
	Самостоятельная работа		**28**	**2, 3**

	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. Зашита авторских прав. Подготовка индивидуального задания по теме «Проблемы обеспечения безопасности ОС. Архитектура подсистемы защиты ОС». Подготовка презентации по криптографии.		
Тема 6.5. Технологии обнаружения вторжений	**Содержание**	**44**	
	1 **Анализ защищенности и обнаружение атак.** Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак.	**2**	**2, 3**
	2 **Защита от вирусов. Методы управления средствами сетевой безопасности.** 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.	**3**	**2, 3**
	Практические занятия		
	1. **Сигнатурный анализ и обнаружение аномалий**	**6**	**2, 3**
	2. **Обнаружение в реальном времени и отложенный анализ.** Локальные и сетевые системы обнаружения атак	**4**	**2, 3**
	3. **Распределенные системы обнаружения атак.** Система обнаружения атак Snort.	**6**	**2, 3**
	Самостоятельная работа Примерная тематика внеаудиторной самостоятельной работы: Службы каталогов. Подготовка индивидуального задания по теме «Аудит информационной безопасности компьютерных систем».	**23**	**2, 3**
Консультации		**4**	
Обязательная аудиторная учебная нагрузка по курсовой работе (проекту) .		**20**	*2,3*
Всего		**260**	

*Внутри каждого раздела указываются соответствующие темы. По каждой теме описывается содержание учебного материала (в дидактических единицах), наименования необходимых лабораторных работ и практических занятий (отдельно по каждому виду), контрольных работ, а также примерная тематика самостоятельной работы. Если предусмотрены курсовые работы (проекты) по дисциплине, описывается примерная тематика. Объем часов определяется по каждой позиции столбца 3 (отмечено звездочкой *). Уровень освоения проставляется напротив дидактических единиц в столбце 4 (отмечено двумя звездочками **).*

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);

2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)

3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия лаборатории программно-аппаратной защиты объектов сетевой инфраструктуры

Оборудование:
Комплект учебной мебели (16 посадочных мест)
Персональный компьютер обучающегося (10 шт.)
Интерактивная доска SMART Board SBM680 (диагональ 77")
Мультимедийный проектор SMART V30
Сетевое оборудование: коммутатор D-Link DES-3200-28/ME

Лицензионное программное обеспечение:
Microsoft Windows 10 Professional 64-bit
(10 лицензий WinPro 10 RUS Upgrd OLP NL Acdmc
Торговый посредник: ООО "Компакт" Номер заказа торгового посредника: MM216912
Дата заказа: 2017-06-16
Код лицензии: 68589678 Родительская программа: OPEN 98645580ZZE1906)
Kaspersky Endpoint Security 10 для Windows
(Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 250-499 Node 2 year Educational Renewal License
№ лицензии: 1096-181214-111355-563-621
Срок использования ПО: с 2018-12-14 до 2021-03-02
Поставщик (реселлер): BENEF.IT Бенефит, ООО)
АСКОН КОМПАС-3D V12 Университетская лицензия с библиотеками и приложениями
(Лицензионное соглашение Кк-10-01408 от 03.12.2010 г. Кол-во копий: 50
Ключ аппаратной защиты HASP HL Net 50 v2 ID 1579998279)
Smart Notebook 17 (лицензия в комплекте с интерактивной доской)

Свободное программное обеспечение:
Libre Office 5.4
Oracle VM VirtualBox
Microsoft Visual Studio Community 2017
Python 3.4
Maxima 5.3.7
Scilab 4.1.2
Cisco Packet Tracer
Pascal ABC.NET

3.2. Информационное обеспечение обучения.

Основные источники:

1.Ковалев, Д.В. Информационная безопасность : учебное пособие : [16+] / Д.В. Ковалев, Е.А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 01.09.2020). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.

Дополнительные источники:

1. Прокушев, Я.Е. Информационная безопасность : практикум / Я.Е. Прокушев. – Санкт-Петербург : ИЦ "Интермедия", 2018. – 288 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=482805 (дата обращения: 01.09.2020). – Библиогр.: с. 282-283. – ISBN 978-5-4383-0168-4. – Текст : электронный.
2. Моргунов, А.В. Информационная безопасность : учебно-методическое пособие : [16+] / А.В. Моргунов ; Новосибирский государственный технический университет. –

Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 01.09.2020). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный.

Программное обеспечение и Интернет-ресурсы:

1. ЭБС «Университетская библиотека онлайн». – Режим доступа: http://biblioclub.ru.
2. Образовательный портал. Режим доступа: Intuit.ru.
3. ЭБС IPRBooks/ - Режим доступа: http://www.iprbookshop.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения по учебной дисциплине	**Формируемые компетенции**	**Оценочные средства по дисциплине**
иметь практический опыт: - обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя; - удаленного администрирования и восстановления работоспособности сетевой инфраструктуры; - организации бесперебойной работы системы по резервному копированию и восстановлению информации; - поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры. **уметь:** - выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; - использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры; - осуществлять диагностику и поиск неисправностей технических средств; - выполнять действия по устранению неисправностей в части, касающейся полномочий техника; - тестировать кабели и коммуникационные устройства;	ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6.	Вопросы для экзамена Тест

- выполнять замену расходных материалов и мелкий ремонт периферийного оборудования; - 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; **знать:** - архитектуру и функции систем управления сетями, стандарты систем управления; - задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией; - средства мониторинга и анализа локальных сетей; - классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; - правила эксплуатации технических средств сетевой инфраструктуры; - расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры; - методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных; - 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.		