ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАБАРДИНО - БАЛКАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Х.М. БЕРБЕКОВА»
КОЛЛЕДЖ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЭКОНОМИКИ

УТВЕРЖДАЮ
Директор колледжа информационных технологий и экономики

_____/ Ф.Б. Нахушева/

«____»_____2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.12 ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Программа подготовки специалистов среднего звена

09.02.05 Прикладная информатика (по отраслям)

Среднее профессиональное образование

Квалификация выпускника
Техник-программист

Очная форма обучения

Нальчик, 2019 г.

Рабочая программа учебной дисциплины ОП.12. Защита информации в компьютерных сетях разработана на основании Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.05 Прикладная информатика (по отраслям), утвержденного приказом Министерства образования и науки Российской Федерации от 13.08.2014 г. № 1001, учебного плана по программе подготовки специалистов среднего звена.

Составители: Оришев Х.Х., Назарова Л.Х.

Рабочая программа учебной дисциплины рассмотренаи одобрена на заседании ЦК Прикладной информатики

Протокол №_ от «___» _____ 2019 г.

Председатель ЦК _____ Назарова Л.Х.

Согласовано

Научная библиотека КБГУ,
отдел комплектования _____ Губжокова Н.А.

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ....4
2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ....6
3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ....10
4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ 12

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.12 ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.05 Прикладная информатика (по отраслям)

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена: учебная дисциплина входит в цикл общепрофессиональных дисциплин.

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

В результате освоения учебной дисциплины обучающийся должен

уметь:

- обеспечивать резервное копирование данных;
- осуществлять меры по защите компьютерных сетей от несанкционированного доступа;
- применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами;
- осуществлять мероприятия по защите персональных данных;
- вести отчетную и техническую документацию.
- организовывать защищенные соединения сетей предприятий, доступ в Интернет и иные.

В результате освоения учебной дисциплины обучающийся должен

знать:

- виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них;
- аппаратные и программные средства резервного копирования данных;
- методы обеспечения защиты компьютерных сетей от несанкционированного доступа;
- специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами;
- состав мероприятий по защите персональных данных;
- защищенные соединения сетей.

Процесс изучения дисциплины направлен на формирование следующих общих и профессиональных компетенций:

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 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 частой смены технологий в профессиональной деятельности.
ПК 1.1. Обрабатывать статический информационный контент.
ПК 1.2. Обрабатывать динамический информационный контент.
ПК 1.3. Осуществлять подготовку оборудования к работе.
ПК 1.4. Настраивать и работать с отраслевым оборудованием обработки информационного контента.
ПК 2.1. Осуществлять сбор и анализ информации для определения потребностей клиента.
ПК 2.3. Проводить отладку и тестирование программного обеспечения отраслевой направленности.
ПК 3.1. Разрешать проблемы совместимости программного обеспечения отраслевой направленности.

1.4. Количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки обучающегося 75 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 50 часов;

самостоятельной работы обучающегося 25 часа.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	75
Обязательная аудиторная учебная нагрузка (всего)	50
в том числе:	
практические занятия	*24*
Самостоятельная работа обучающегося	25
Промежуточная аттестация в форме дифференцированного зачета	

2.2.Тематический план и содержание учебной дисциплины ОП.12 Защита информации в компьютерных сетях

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)		Объем часов	Уровень освоения
1	2		3	4
Раздел 1.	**Обеспечение информационной безопасности ПК и компьютерных сетей**			
Тема 1.1 Виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей	**Содержание учебного материала**		8	
	1.	**Основные понятия защиты информации.** Защита информации от несанкционированного доступа (НСД). Система защиты информации		1,2
	2	**Понятие информационной безопасности (ИБ).** Понятие автоматизированных систем (АС). Компоненты АС. Конфиденциальность данных. Целостность данных. Виды угроз. Классификация угроз.		1,2
	3	**Использование сети Интернет.** Модель ISO/OSI и стек протоколов TCP/IP. Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.		1,2
	4	**Способы обеспечения ИБ сетей.** Пути решений проблем защиты информации в сетях. Задачи управления системой сетевой безопасности.		1,2
	Практическая работа №1 «Работа с шифрующей файловой системой EFS и управление сертификатами. Настройка параметров аутентификации».		2	2
	Самостоятельная работа Защита информации от несанкционированного доступа Угрозы и уязвимости проводных корпоративных сетей		4	3
Тема 1.2.Аппаратные и программные средства резервного копирования данных	**Содержание учебного материала**		3	
	1.	**Аппаратные и программные средства резервного копирования данных.** Классификация программ резервного копирования. Краткий обзор наиболее популярных программ резервного копирования. Сравнение программ резервного копирования. Аппаратные средства резервного копирования		1,2
	Практическая работа №2 «Создание резервной копии системы с помощью стандартных программ. Восстановление системы из резервной копии»		2	2
	Практическая работа №3 «Создание резервной копии системы с помощью Acronis. Восстановление системы и данных с помощью Acronis»		2	
	Самостоятельная работа Модели безопасности по разграничению доступа в систему Модели защиты при отказе в обслуживании		5	3
	Рубежный контроль №1		1	3
Тема 1.3 Методы обеспечения защиты компьютерных сетей от	**Содержание учебного материала**		2	
	1.	**Стратегия предотвращения несанкционированного доступа в информационную систему (ИС).** Модели безопасности по разграничению доступа в систему. Модели контроля целостности информации в системе. Модели защиты при отказе в обслуживании. Модели анализа безопасности ПО. Модель безопасности объектов ВС.		1,2

несанкционированного доступа	2.	**Понятия политики безопасности.** Обеспечение ИБ в нормальных ситуациях. Обеспечение ИБ в чрезвычайных ситуациях. Описание проблемы. Область применения. Позиция организации. Распределение ролей и обязанностей. Администраторы локальной сети	2	1,2
	Практическая работа №4 Разграничение прав пользователей. Защита от несанкционированного доступа и сетевых хакерских атак		2	2
	Практическая работа №5 Назначение прав пользователей при произвольном управлении доступом. Разграничение доступа к ресурсам		2	
	Практическая работа №6 Реализация политики безопасности		2	
	Самостоятельная работа Модели безопасности по разграничению доступа в систему Модель безопасности объектов ВС		6	3
Тема 1.4 Специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами	**Содержание учебного материала**		6	
	1.	**Классификация компьютерных вирусов.** Жизненный цикл вирусов. Классические способы распространения Электронная почта. Троянские Web-сайты		1,2
	2	**Методы обнаружения вирусов.** Антивирусные программы. Антивирусные комплексы. Встраивание антивирусов в BIOS компьютеров. Виды антивирусных программ Профилактические меры защиты. Построение системы антивирусной защиты корпоративной сети. Защищенные соединения сетей		1,2
	Практическая работа №7 Проверка компьютера на вирусы с помощью антивирусной программы Avira Anti Vir PersonalEditionClassic Установка программы Avira Anti VirPersonalEditionClassic		2	2
	Практическая работа №8 Проверка работы антивирусного сторожа. Проверка работы антивирусного сканера		2	
	Практическая работа №9 Восстановление зараженных файлов. Профилактика «троянских программ». Организация защищенных соединений сетей предприятий, доступ в Интернет и иные».		2	
	Практическая работа №10 Установка и предварительная настройка Антивируса Касперского Работа с Антивирусом Касперского.		2	
	Практическая работа №11 Выявление вредоносных программ. Выявление вредоносных программ с помощью командной строки		4	
	Самостоятельная работа Классификация компьютерных вирусов Политики безопасности Виды антивирусных программ		7	3
Тема 1.5 Состав мероприятий по защите персональных данных	**Содержание**		2	
	1.	**Состав мероприятий по защите персональных данных** Основные мероприятия обеспечения безопасности персональных данных. Мероприятия по техническому обеспечению безопасности персональных данных		1,2
	Самостоятельная работа Построение системы антивирусной защиты корпоративной сети		3	3
	Рубежный контроль №2		1	3
	Дифференцированный зачет		1	3
		Всего	**75**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению.

Реализация учебной дисциплины требует наличия учебного кабинета.

Технических средств обучения:

- интерактивная доска;
- проектор;
- источник бесперебойного питания;
- аудиторная доска;
- демонстрационные печатные пособия и демонстрационные ресурсы в электронном представлении.

Оборудование лаборатории и рабочих мест лаборатории: компьютерный класс с выходом в Интернет, оснащенный методическими и справочными материалами, наглядными пособиями, нормативной документацией, программным обеспечением и других современных технологий.

3.2.Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. — Электрон. текстовые данные. — Саратов : Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

2. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Электрон. текстовые данные. — М. : Евразийский открытый институт, 2012. — 311 c. — 978-5-374-00301-7. — Режим доступа: http://www.iprbookshop.ru/10677.html

3. Качановский, Ю. П. Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами [Электронный ресурс] : методические указания к проведению лабораторной работы по курсу «Информатика» / Ю. П. Качановский, А. С. Широков. — Электрон. текстовые данные. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2014. — 24 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/55120.html

Дополнительные источники:

1. Ермаков, Д. Г. Применение антивирусных программ для обеспечения информационной безопасности [Электронный ресурс] / Д. Г. Ермаков, А. В. Присяжный. — Электрон. текстовые данные. — Екатеринбург : Уральский федеральный университет, ЭБС АСВ, 2013. — 64 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/66577.html

2. Лабораторный практикум по дисциплине Методы и средства защиты информации в компьютерных сетях [Электронный ресурс] / сост. А. Г. Симонян Т. Б. К. Режеб. — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 58 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61742.html

Интернет-ресурсы:

1. http://www.itsec.ru/
2. http://www.securitylab.ru/
3. http://www.iprbookshop.ru/

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения учебной дисциплины обучающийся должен уметь: обеспечивать резервное копирование данных; осуществлять меры по защите компьютерных сетей от несанкционированного доступа; применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами; осуществлять мероприятия по защите персональных данных; вести отчетную и техническую документацию. организовывать защищенные соединения сетей предприятий, доступ в Интернет и иные. В результате освоения учебной дисциплины обучающийся должен знать**:** виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них; аппаратные и программные средства резервного копирования данных; методы обеспечения защиты компьютерных сетей от несанкционированного доступа; специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами; состав мероприятий по защите персональных данных; защищенные соединения сетей.	Контроль усвоения знаний проводится в форме контрольной работы. Контроль формирования умений производится в форме защиты практических работ. Промежуточная аттестация по дисциплине проходит в соответствии с учебным планом по специальности. Критерием оценки результатов освоения дисциплины является способность выполнения конкретных профессиональных задач, во время учебной и производственной практики: - планирование и самостоятельное выполнение деятельности, решение проблемных задач; - выполнение деятельности по образцу, инструкции или под руководством; - узнавание ранее изученных объектов, свойств.