государственное автономное учреждение
Калининградской области
профессиональная образовательная организация
«КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ 03

Обеспечение информационной безопасности компьютерных сетей

2021

СОГЛАСОВАНО

Зам. директора по УМР

_____ Ю.И. Бурыкина

УТВЕРЖДАЮ

Директор ГАУ КО

«Колледж предпринимательства»

_____ Л.Н. Коцева

«30» __июня__2021г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности **09.01.02 Наладчик компьютерных сетей**

Организация-разработчик: государственное автономное учреждение Калининградской области профессиональная образовательная организация «Колледж предпринимательства»

Разработчики:

Зверев М.В. - ГАУ КО «Колледж предпринимательства», преподаватель

Рабочая программа учебной дисциплины рассмотрена на заседании отделения информационных технологий. Протокол № 6 от 30.06.2021 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Организация и управление торгово-сбытовой деятельностью

1.1. Область применения программы

Рабочая программа профессионального модуля является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности **09.01.02 Наладчик компьютерных сетей** базовой подготовки, в части освоения основного вида деятельности: **Обеспечение информационной безопасности компьютерных сетей** и соответствующих профессиональных компетенций (ПК).

1.2. Цели и задачи модуля – требования к результатам освоения модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности - Обеспечение информационной безопасности компьютерных сетей

и соответствующие ему общие компетенции, и профессиональные компетенции:

Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранных языках.
ОК 11	Планировать предпринимательскую деятельность в профессиональной сфере

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ПК 3.1	Обеспечить резервное копирование данных.
ПК 3.2	Осуществлять меры по защите компьютерных сетей от несанкционированного доступа.
ПК 3.3	Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.
ПК 3.4	Осуществлять мероприятия по защите персональных данных.

В результате освоения профессионального модуля студент должен:

Иметь практический опыт	- обеспечения информационной безопасности компьютерных сетей, резервного копирования и восстановления данных; - установки, настройки и эксплуатации антивирусных программ; - противодействия возможным угрозам информационной безопасности;
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;
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.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

максимальной учебной нагрузки обучающегося – 841 часа, включая:
обязательной аудиторной учебной нагрузки обучающегося – 238 часа;
самостоятельной работы обучающегося – 99 час;
учебной практики – 72 часа;
производственной практики – 432 часа.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности Выполнение работ по монтажу, наладке, эксплуатации и обслуживанию локальных компьютерных сетей и соответствующих профессиональных компетенций, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранных языках.
ОК 11	Планировать предпринимательскую деятельность в профессиональной сфере
ПК 3.1	Обеспечить резервное копирование данных.
ПК 3.2	Осуществлять меры по защите компьютерных сетей от несанкционированного доступа.
ПК 3.3	Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.
ПК 3.4	Осуществлять мероприятия по защите персональных данных.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	**Наименования разделов профессионального модуля[1]***	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., курсовая работа (проект),** часов		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ПК 1.1.- ПК 1.5.	МДК 03.01 Информационная безопасность ПЭВМ и компьютерных сетей	337	238	110	-	110	-	-	-
	Производственная практика, часов *(если предусмотрена итоговая (концентрированная)*		-						-
	Всего	337							

1

3.2. Содержание обучения по профессиональному модулю

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объём, часов	Уровень освоения
1	**2**	**3**	**4**
ПМ.03 Обеспечение информационной безопасности компьютерных сетей			
МДК 03.01. Информационная безопасность ПЭВМ и компьютерных сетей		**337**	
Раздел 1. Защита информации		**172**	
Тема 1.1. Виды угроз и методы защиты персональных компьютеров, серверов и корпоративных сетей от них.	**Содержание учебного материала**	12	1
	1. Определение угроз и анализ рисков.		
	2. Модели и методы защиты ПК от вирусов и от несанкционированного доступа.		
	3. Защита серверов и корпоративных сетей от угроз.		
	4. Антивирусные программы		
	5. Троянские программы. Защита ПК.		
	6. Принципы работы межсетевых экранов. Пакеты межсетевых экранов		
	Практические занятия.	30	
	Практическое занятие №1. Определение угроз		
	Практическое занятие №2. Анализ рисков		
	Практическое занятие №3. Построение модели защиты ПК и сети от вирусов		
	Практическое занятие №4. Выбор метода защиты ПК от вирусов и от несанкционированного доступа.		
	Практическое занятие №5. Установка безопасности Windows		
	Практическое занятие №6. Установка и настройка антивирусного ПО		
	Практическое занятие №7.Обновление антивирусного ПО		

	Практическое занятие №8. Отключение и удаление неиспользованных учетных записей		
	Практическое занятие №9. Установка паролей для всех учетных записей пользователей		
	Практическое занятие №10. Защита сервера от вирусов		
	Практическое занятие №11. Диагностика заражения ПК вирусами. Контроль карантина.		
	Практическое занятие №12. Восстановление зараженных файлов, папок.		
	Практическое занятие №13. Установка и настройка межсетевого экрана		
	Практическое занятие №14. Защита корпоративных сетей от вирусов и троянских программ		
	Практическое занятие №15. Настройка пакетов межсетевого экрана.		
Тема 1.2. Аппаратные и программные средства резервного копирования данных	**Содержание учебного материала:**	20	2
	7. Аппаратные средства резервного копирования данных.		
	8. Программные средства резервного копирования.		
	9. Виды резервного копирования. Разработка и реализация стратегии резервного копирования.		
	10. Понятие плана архивации. Выбор архивных устройств и носителей		
	11. Примеры построения систем резервного копирования		
	12. Теневые копии		
	13. Технология хранения резервных копий		
	14. Способы резервного копирования перед и после обновления системы.		
	15. Создание ASR-копии.		
	16. Алгоритмы резервного копирования		
	Практические занятия	30	2
	Практическое занятие №16. Установка и настройка аппаратных средств резервного копирования данных		
	Практическое занятие №17. Установка и настройка программных средств резервного копирования данных		
	Практическое занятие №18. Разработка и реализация стратегии резервного копирования.		

	Практическое занятие №19. Резервное копирование данных.		
	Практическое занятие №20. Архивирование данных		
	Практическое занятие №21. Выбор архивных устройств и носителей		
	Практическое занятие №22. Определение ограничений для резервного копирования.		
	Практическое занятие №23. Теневые копии		
	Практическое занятие №24. Обновление ПО для резервного копирования данных.		
	Практическое занятие №25. Резервное копирование перед и после обновления системы.		
	Практическое занятие №26. Создание ASR-копии		
	Практическое занятие №27. Установка приемлемого окна резервного копирования данных.		
	Практическое занятие №28. Установка расписания резервного копирования данных.		
	Практическое занятие №29. Разработка политики хранения резервных копий.		
	Практическое занятие №30. Описание процесса создания резервной копии.		
Тема 1.3. Состав мероприятий по защите персональных данных	**Содержание учебного материала**	8	
	17. Соблюдение законодательства в области защиты персональных данных		
	18. Состав мероприятий по защите персональных данных		
	19. Перечень мероприятий по защите персональных данных		
	20. Мероприятия по техническому обеспечению безопасности персональных данных при обработке в информационных системах		
	Практические занятия	24	2
	Практическое занятие №31. Архитектура безопасности данных.		
	Практическое занятие №32. Классификация информационных систем персональных данных		
	Практическое занятие №33. Защита информации от утечки по техническим каналам		
	Практическое занятие №34. Защита информации от несанкционированного доступа		
	Практическое занятие №35. Межсетевые экраны на границе контролируемой зоны ИСПДн		
	Практическое занятие №36. Шифрование данных и файлов		
	Практическое занятие №37. Непрерывное обеспечение безопасности данных.		

	Практическое занятие №38. Организация и проведение мероприятий по защите персональных данных		
	Практическое занятие №39. Создание системы защиты персональных данных		
	Практическое занятие №40. Приведение процессов обработки и обеспечения безопасности персональных данных в соответствие требованиям законодательства		
	Практическое занятие №41. Реализация политик шифрования данных в состоянии покоя		
Тема 1.4. Восстановление БД и управление доступом БД	**Содержание учебного материала**	20	2
	21. Основные сведения об архитектуре БД.		
	22. Управление доступом БД.		
	23. Программы и методы проверки подлинности.		
	24. Авторизация пользователей. Добавление пользователей БД.		
	25. Разрешения назначаемые на уровне БД.		
	26. Создание и управление учетными записями.		
	27. Доступ к БД		
	28. Информационная безопасность систем управления БД.		
	29. Восстановление БД. Программы восстановления.		
	30. Информационная безопасность систем управления БД.		
	Практические занятия	28	2
	Практическое занятие №42. Архитектура БД		
	Практическое занятие №43. Восстановление данных из резервной копии.		
	Практическое занятие №44. Установка программ для проверки подлинности.		
	Практическое занятие №45. Выбор методов проверки подлинности.		
	Практическое занятие №46. Проверка подлинности.		
	Практическое занятие №47. Авторизация пользователей		
	Практическое занятие №48. Добавление пользователей БД.		
	Практическое занятие №49. Назначение решений на уровне БД.		
	Практическое занятие №50. Создание учетных записей.		
	Практическое занятие №51. Управление учетными записями.		
	Практическое занятие №52. Управление доступом БД.		
	Практическое занятие №53. Работа с учетными записями.		
	Практическое занятие №54. Осуществление доступа к БД		

	Практическое занятие №55. Работа с программами восстановления данных.		
Раздел 2 Обеспечение сетевой и компьютерной безопасности.		**68**	
Тема 2.1. Методы обеспечения защиты компьютерных сетей от несанкционированного доступа	**Содержание учебного материала**	36	
	31. Проблемы несанкционированного доступа.		
	32. Средства ограничения физического доступа.		
	33. Средства защиты от НСД по сети.		
	34.Современная технология и криптография защиты данных в сети		
	35. Сетевой монитор безопасности.		
	36. Безопасность ресурсов и контроль доступа		
	37. Сканирование уязвимостей.		
	38. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.		
	39. Основные этапы допуска к ресурсам вычислительной системы.		
	40. Допуск к ресурсам сети		
	41. Допуск к ресурсам сервера, базы данных		
	42. Использование динамически изменяющегося пароля.		
	43. Взаимная проверка подлинности и другие случаи опознания.		
	44. Применение различных способов разграничения доступа к компьютерным ресурсам.		
	45. Разграничение доступа по спискам.		
	46. Способы защиты по локальной сети		
	47. Настройки доступа локальной сети		
	48. Программное обеспечение обеспечивающее защиту компьютерных сетей от несанкционированного доступа		
Тема 2.2. Специализированые средства борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.	**Содержание учебного материала**	32	2
	49. Программы-детекторы		
	50. Программы-доктора и ревизоры		
	51. Программы-фильтры		
	52. Спам. Виды спама. Способы распространения спама.		
	53. Архитектура серверных систем фильтрации спама.		
	54. Антивирусные программы.		
	55. Борьба со спамом техническими средствами.		

	56. Фильтрация почты.		
	57. Сбор адресов электронной почты.		
	58. Создание черных списков		
	59. Авторизация почтовых серверов		
	60. Сортировка писем.		
	61. Использование антивирусной защиты при заражении ПК.		
	62. Автоматическое шифрование логических дисков ПК.		
	63. Использование матрицы установления полномочий		
	64. Произвольное и принудительное управление доступом.		
	Всего	**238**	
Самостоятельная работа при изучении ПМ.02 Систематическая проработка конспектов занятий, учебной и специальной технической литературы с целью выполнения заданий преподавателя. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, подготовка к их защите. Написание рефератов по темам: «Понятие «информационная система безопасности»», «Виды интерфейсов», «Уникальные адреса для провайдера», «Обзор маршрутизаторов и схем маршрутизации», «Сеанс BGP. Настройка параметров», «Пассивное сетевое оборудование», «Роль прокси-серверов в обработке запросов и ответов HTTP», «Основы передачи данных в беспроводных сетях с учетом безопасности», «Клиентское и серверное программное обеспечение сети Интернет», «Эволюция и функции браузеров», «Временная локализация»		99	
	Итого	**337**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие учебных кабинетов информатики и информационных технологий; - учебных кабинета: информатики и информационных технологий;

- кабинет информатики и информационных технологий;
- лабораторий электротехники с основами радиоэлектроники

Оборудование учебного кабинета и рабочих мест кабинета информатики и информационных технологий;

- рабочие места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-методических материалов, методические рекомендации и разработки;
- учебно-методические пособия на CD/DVD - дисках;
- видеоматериалы по ремонту и устройству оборудования;
- плакаты по устройству различного оборудования;
- образцы инструментов, приспособлений;
- измерительные приборы и тестовые разъемы для проверки портов ПК;
- макеты аппаратных частей вычислительной техники и оргтехники.

Технические средства обучения: персональный компьютер с лицензионным программным обеспечением и мультимедиапроектор. Рабочие станции с выходом в интернет и сервер. Локальная сеть. Коммуникаторы.

Реализация программы модуля предполагает обязательную производственную практику.

4.2. Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники для студентов:

1.Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учеб.пособие/ О.Р. Лапонина; под.ред. В.А. Сухомлина.- 2 е изд., испр.-М.: Интернет – Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 201. – 531с.

2. Б.А. Фороузан. Криптография и безопасность сетей: учебное пособие; пер. с англ.под ред. А.Н. Берлина – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010.- 784с.

3. Создание защищённых беспроводных сетей 802.11 в MS Windows. Справочник профессионала./ пер.с англ. – М.: Издат-во «ЭКОМ», 2006г. 400с.

4. Б. Роберта. Безопасность сетей. Полное руковод-во, Р.Брэгг, М. Родс-Оусли, пер. с англ.- М.: Издат-во «ЭКОМ», 2011. – 912с.:ил.

5. Безопасность сетей. Практ. Пособие. Пер. с англ. – М.: ЭКОМ Паблишерз, 2011. – 528с.

Основные источники для преподавателей:

1.Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учеб.пособие/ О.Р. Лапонина; под.ред. В.А. Сухомлина.- 2 е изд., испр.-М.: Интернет – Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 201. – 531с.

2. Б.А. Фороузан. Криптография и безопасность сетей: учебное пособие; пер. с англ.под ред. А.Н. Берлина – М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010.- 784с.

3. Создание защищённых беспроводных сетей 802.11 в MS Windows. Справочник профессионала./ пер.с англ. – М.: Издат-во «ЭКОМ», 2006г. 400с.

4. Б. Роберта. Безопасность сетей. Полное руковод-во, Р.Брэгг, М. Родс-Оусли, пер. с англ.- М.: Издат-во «ЭКОМ», 2011. – 912с.:ил.

5. Безопасность сетей. Практ. Пособие. Пер. с англ. – М.: ЭКОМ Паблишерз, 2011. – 528с.

Интернет ресурсы:

http://kubok.yandex.ru

http://www.fid.ru/museum

http://www.nethistory.ru

http://www.allbest.ru

http://www.remont-nastroyka-pc.ru.

http://school-collection.edu.ru/catalog/

http://www.wikiznanie.ru

Интернет-университет информационных технологий (ИНТУИТ.ру) http://www.intuit.ru

Дополнительные источники (при необходимости)

1.Приводится тематика дополнительных образовательных и информационных ресурсов, разработка которых желательная для освоения данного модуля.

4.3. Общие требования к организации образовательного процесса

Освоение программы модуля базируется на изучении общепрофессиональных дисциплин: «Основы информационных технологий», «Основы электротехники», «Охрана труда и техника безопасности».

Реализация программы модуля предполагает выполнение обучающимися практических работ, включая как обязательный компонент практические задания с использованием персональных компьютеров, оснащенных лицензионным программным обеспечением общего и профессионального назначения.

Реализация программы модуля предполагает концентрированную учебную практику.

Выполнение практических занятий предполагает деление группы по числу рабочих мест, оборудованных персональным компьютером.

В процессе обучения используются различные виды информационнокоммуникационных технологий.

Консультации обучающихся проводятся согласно графику консультаций, составленному учебным заведением.

Текущий контроль освоения содержания МДК осуществляется в форме тестовых заданий и практических занятий.

Формой аттестации МДК 03.01. является экзамен.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу: наличие высшего профессионального образования, соответствующего профилю преподаваемого модуля «Ввод и обработка цифровой информации».

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: мастера производственного обучения должны иметь на 1 - 2 разряда по профессии рабочего выше, чем предусмотрено образовательным стандартом для выпускников.

Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального цикла, эти преподаватели и мастера производственного обучения должны проходить стажировку в профильных организациях не реже 1-го раза в 3 года.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 3.1. Обеспечение резервного копирование данных.	-соблюдение этапов резервного копирования данных; - обоснованный выбор данных предназначенных для резервного копирования; - использование аппаратных и программных средств резервного копирования данных.	Экспертная оценка деятельности обучающихся в рамках учебной и производственной практик. Экспертная оценка защиты практических занятий
ПК 3.2. Осуществлять меры по защите компьютерных сетей от несанкционированного доступа.	- использование специализированных средств для борьбы с вирусами; -соблюдение методов обеспечения по защите компьютерных сетей от несанкционированного доступа; - принятие мероприятий по защите персональных данных.	Экспертная оценка защиты практических занятий. Экспертная оценка тестирования обучающихся.
ПК 3.3. Применение специализированных средств для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами.	- выполнение требований по защите компьютерных сетей от несанкционированного доступа; -применение специализированных средств для борьбы с вирусами; - соблюдение мер по защите от несанкционированных рассылок электронной почты вредоносными программами	Экспертная оценка защиты практических занятий. Экспертная оценка устного опроса обучающихся.
ПК 3.4. Осуществлять мероприятия по защите персональных данных.	-осуществление мероприятий по защите персональных данных; -соблюдение основных этапов установки и настройки программ по защите данных.	Экспертная оценка защиты практических занятий. Экспертная оценка письменного опроса обучающихся.

ПК 3.5. *Восстанавливать БД и управлять доступом к БД*	- восстановление ДБ; - управление доступом	Экспертная оценка защиты практических занятий. Экспертная оценка тестирования обучающихся.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	Основные показатели результатов подготовки	Формы и методы контроля
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	-обоснование сущности и социальной значимости своей будущей профессии; -добросовестное выполнение учебных обязанностей при освоении профессиональной деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося процессе освоения образовательной программы
ОК 2. Организовывать Собственную деятельность, исходя из цели и способов ее достижения, определенных руководителем.	-обоснованный выбор и применение методов и способов решения профессиональных задач в области установки и обслуживании программного обеспечения вычислительной техники; -правильная последовательность выполнения действий на лабораторных, практических работах, во время учебной и производственной практик в соответствии с инструкциями, указаниями и т.п.	Наблюдение и экспертная оценка на практических и лабораторных занятиях, при выполнении работ по учебной и производственной практикам
ОК 3. Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.	-демонстрация способности принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. -полнота представлений за последствия некачественно и несвоевременно выполненной работы	Наблюдение и экспертная оценка эффективности и правильности самоанализа принимаемых решений на практических занятиях, в процессе учебной и производственной практик

ОК 4. Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач	- демонстрация приемов и способов работы с различными информационными источниками (учебной, справочной, технической литературой) для эффективного выполнения профессиональных задач	Наблюдение и экспертная оценка на практических и лабораторных занятиях, при выполнении работ по учебной и производственной практикам
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	-демонстрация навыков получения информации из электронных учебников, обучающих программ. -демонстрация навыков использования Интернет-ресурсов в профессиональной деятельности.	Наблюдение и экспертная оценка на практических и лабораторных занятиях, при выполнении работ по учебной и производственной практикам
ОК 6. Работать в команде, эффективно общаться с коллегами, руководством, клиентами.	-корректное взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения; -полнота понимания того, что успешность и результативность работы зависит от согласованности действий всех участников команды работающих;	интерпретация результатов наблюдения за деятельностью обучающегося в ситуациях взаимодействия
ОК 7. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).	- демонстрация готовности к исполнению воинской обязанности; -самостоятельный выбор учетно-военной специальности, родственной полученной профессии	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.