

*к ООП по специальности
09.02.06 Сетевое и системное администрирование*

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
Государственное бюджетное профессиональное образовательное учреждение
Московской области «Электростальский колледж»**

Утверждена приказом руководителя
образовательной организации
№ 211-од от 23.05. 2023 года

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ. 03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ
ИНФРАСТРУКТУРЫ**

г.о.Электросталь, 2023 г.

РАССМОТРЕНО

ПЦК профессионального,
цикла по специальности

09.02.06 Сетевое и системное администрирование

Протокол № 10

«13» мая 2023 г.

Председатель ПЦК /Черкасов Н.В./

Рабочая программа профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры разработана на основании:

1. Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование, утвержденного приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г. N 1548 (регистрационный номер 44978 от 23.12.2016г.)

3. Федерального закона от 31 июля 2020 г. №304-ФЗ «О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся

4. Учебного плана по специальности 09.02.06 Сетевое и системное администрирование, утвержденного 23 мая 2023 года, приказ № 211-од

Организация-разработчик: ГБПОУ МО «Электростальский колледж»

Автор программы: Черкасов Николай Владимирович, преподаватель
Фамилия И.О., должность, подпись

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	6
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	25

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03. ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

1.1. Область применения программы

Рабочая программа профессионального модуля (далее программа) - является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.06 **Сетевое и системное администрирование** (в части освоения основного вида профессиональной деятельности (ВПД): **Эксплуатация объектов сетевой инфраструктуры** и соответствующих профессиональных компетенций (ПК):

1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программноаппаратные средства компьютерных сетей;
2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях;
3. Эксплуатировать сетевые конфигурации;
4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации;
5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования;
6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Программа профессионального модуля может быть использована в дополнительном профессиональном образовании (курсы повышения квалификации и переподготовки), а также для всех форм получения образования: очной, очно - заочной (вечерней) и экстерната, для всех типов и видов образовательных учреждений, реализующих ОПОП СПО по специальности 09.02.06 Сетевое и системное администрирование. Цели и задачи модуля - требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности с соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен: *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 программноаппаратных 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 (ИС), 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.

Наименование разделов профессионального модуля (междисциплинарных курсов):

МДК.03.01. Эксплуатация объектов сетевой инфраструктуры;

МДК.03.02. Безопасность функционирования информационных систем;

Виды промежуточной аттестации:

- экзамен квалификационный по профессиональному модулю
- экзамен по каждому междисциплинарному курсу;
- дифференциальный зачет по практике (учебной и производственной).

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности *Сопровождение, настройка и администрирование системного и сетевого программного обеспечения, эксплуатация и обслуживание серверного и сетевого оборудования, диагностика и обеспечение целостности и информационной безопасности объектов сетевой инфраструктуры*, в том числе профессиональными (ПК) и общими (ОК) компетенциями

Код	Наименование результата обучения
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.	Эксплуатировать сетевые конфигурации
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 поступившего из ремонта оборудования
ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК.10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК.11	Планировать предпринимательскую деятельность в профессиональной сфере.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	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 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6	МДК.03.01. Эксплуатация объектов сетевой инфраструктуры	403	191	192	-	20	-	252	-
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6	МДК.03.02. Безопасность функционирования информационных систем	115	42	37	30	6	20		-
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6	Производственная практика (по профилю специальности), часов	576							324
	Всего:	1094	233	229	30	26	252	324	

3.2. Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Эксплуатация объектов сетевой инфраструктуры			
МДК 03.01. Эксплуатация объектов сетевой инфраструктуры		403	
Тема 1.1. Эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей	Содержание	191	
	1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети; активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.		2
	2. Логические (информационные) аспекты эксплуатации. Несанкционированное ПО (в том числе сетевое); паразитная нагрузка.		2
	3. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб); наращивание длины сегментов сети; замена существующей аппаратуры (на более мощную). Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.		2
	4. Техническая и проектная документация. Паспорт технических устройств; руководство по эксплуатации; Физическая карта всей сети; логическая схема компьютерной сети;		2
	5. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры Комплекс организационно-технических мероприятий; выявление и своевременная замена элементов инфраструктуры.		2
	6. Проверка объектов сетевой инфраструктуры и профилактические работы Проверка физических компонентов; проверка документации и требований; проверка списка совместимого оборудования.		2
	7. Проведение регулярного резервирования Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения.		2
	8. Анализаторы протоколов Программные или аппаратно-программные системы, функции мониторинга, анализ трафика в сетях.		2
9. Оборудование для диагностики и сертификации кабельных систем	2		

10.	Экспертные системы	2
11	Встроенные системы диагностики и управления. Сетевые мониторы	2
12	Резервное копирование данных	2
13	Хранилищ данных	2
14	Технологии управления информацией. OLAP-технология	2
15	Понятие баз данных.	2
16	Принципы планирования восстановления работоспособности сети при аварийной ситуации	2
17	Допущения при разработке схемы послеаварийного восстановления. Основные требования к политике организации схемы послеаварийного восстановления	2
18	Организация работ по восстановлению функционирования системы	2
19	План восстановления системы Порядок уведомления о чрезвычайных событиях. Активация. Возврат к нормальному функционированию системы.	2
20	Принципы локализации неисправностей	2
21	Контрольно-измерительная аппаратура	2
22	Сервисные платы и комплексы	2
23	Программные средства диагностики	2
24	Номенклатура и особенности работы тест-программ	2
25	Диагностика неисправностей средств сетевых коммуникаций	2
26	Контроль функционирования аппаратно-программных комплексов	2
27	Действия при не работающей сети, при медленной сети,	2
28	Действия при нестабильно работающей сети.	2
29	Архитектура системы управления. Структура системы управления.	2
30	Уровни управления	2
31	Области управления.	2
32	Протоколы управления.	2
33	Управление отказами.	2
34	Учет работы сети. Управление конфигурацией.	2
35	Управление производительностью, безопасностью сети.	2
Практические работы		192
1.	Поддержка пользователей сети.	
2.	Создание пользователей в domain, редактирование пользователей в domain, создание пароля пользователем в domain, создание групп и распределение пользователей по группам в domain.	
3.	Настройка прав доступа.	

4.	Оформление технической документации, правила оформления документов.
5.	Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.
6.	Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.
7.	Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы, коммутационное оборудование)
8.	Вкладка. Сеть утилиты. Диспетчер задач
9.	Использование консоли. Производительность
10	Мониторинг сетевого трафика с помощью утилиты Netstat
11	Тестирование кабелей
12	Тестирование коммутационного оборудования
13	Операции по резервному копированию данных;
14	Операции по восстановлению данных.
15	Организации по бесперебойной работе системы по резервному копированию
16	Восстановление информации
17	Восстановление работоспособности сети после сбоя
18	Разработка плана восстановления
19	Использовать схему после аварийного восстановления сети.
20	Возврат к нормальному функционированию системы.
21	Работа контрольно-измерительной аппаратуры
22	Замена расходных материалов
23	Мелкий ремонт периферийного оборудования
24	Программная диагностика неисправностей
25	Аппаратная диагностика неисправностей
26	Поиск неисправностей технических средств

27	Выполнение действий по устранению неисправностей		
28	Установка программного обеспечения		
29	Анализ сетевого трафика средствами Сетевого монитора		
30	Основные сведения о сетевом мониторе		
31	Запись данных средствами Сетевого монитора		
32	Устранение неполадок с помощью Ping и PathPing		
33	Диагностика сети и Netdiag		
34	Удаленное администрирование;		
35	Восстановление работоспособности сетевой инфраструктуры. Авторизация подключений удаленного доступа		
	Самостоятельная работа при изучении раздела ПМ	20	
	Самостоятельная работа		
	Физическая инфраструктура; Логическая инфраструктура; Сетевые подключения, протоколы, адресация, система имен. Автоматическое назначение частных IP-адресов; Маршрутизация и инфраструктура сети Windows Server 2003; Установка сетевых компонентов Windows; Установка Active Directory в сети Windows; Разбиение на подсети; Механизм разбиения на подсети; Определение емкости подсети; Технические регламенты, виды документов для технических осмотров, методы и принципы проверки различного оборудования, методы резервирования, программы для резервирования информации, BackUp. Маршрутизация в Windows Server 2003; Управление общими свойствами IP-маршрутизации; Основные сведения о NAT; Различие между NAT и ICS; Удаленный доступ по телефонной линии; Авторизация подключений удаленного доступа Основные сведения о политиках удаленного доступа Устранение неполадок при подключениях удаленного доступа Реализация процедур		

	<p>безопасного администрирования сети Оснастка Шаблоны безопасности Схемы обжимки витой пары; Устройство «пакета», передаваемого по сети. Использование бесклассовой междоменной маршрутизации; Маски подсети переменной длины; Проверка существующего IP-адреса; Ручная настройка адреса; DNS; NetBIOS; DNS в сетях Windows Server 2003; Механизм работы DNS-запросов; Настройка параметров DNS-сервера; Средства устранения неполадок DNS; Изучение утилиты Acronis, изучение безопасной зоны Acronis,</p>		
--	---	--	--

Раздел 2. Безопасность функционирования информационных систем

МДК 03.02. Безопасность функционирования информационных систем

		115	
Тема 2.1 Основы информационной сности	Содержание	16	
	1 Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.		2
	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.		2
	3 Государственная информационная политика. Основные положения государственной информационной политики Российской Федерации. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.		2
	4 Информация - наиболее ценный ресурс современного общества. Понятие «информационный ресурс». Классы информационных ресурсов.		2
	5 Проблемы информационной войны. Информационное оружие и его классификация. Информационная война.		2
	6 Проблемы информационной безопасности в сфере государственного и муниципального управления.		2

	7	Информационные системы. Общие положения. Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах.		2	
	8	Методы и модели оценки уязвимости информации. Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза - защита»		2	
	Практические работы		12		
	1	Установка программы Etherreal и подготовка к захвату.			
	2	Пользовательский интерфейс программы Etherreal. Фильтр отображения пакетов. Поиск кадров.			
	3	Выделение ключевых кадров. Сохранение данных захвата. Печать информации. Просмотр кадра в отдельном окне.			
	4	Анализ протоколов Ethernet и ARP.			
	5	Анализ протоколов IP и ICMP.			
	6	Анализ протокола TCP			
	Тема 2.2. Проблемы информационной безопасности	Содержание		8	2
		1	Основные понятия и анализ угроз информационной безопасности. Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.		2
		2	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Анализ угроз сетевой безопасности. Обеспечение информационной безопасности сетей.		2
3		Политика безопасности. Основные понятия политики безопасности. Структура политики безопасности организации.	2		
4		Стандарты информационной безопасности. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий	2		
Практические работы		10			
1				Система анализа рисков проверки политики информационной безопасности предприятия.	
2				Анализ угроз сетевой безопасности.	
3				Этапы сетевой атаки. Исследование сетевой топологии.	
4				Обнаружение доступных сетевых служб. Выявление уязвимых мест атакуемой системы	
5	Реализации атак. Выявление атаки на протокол SMB.				

Тема 2.3. Технологии защиты данных	Содержание		6	2	
	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.			
	2	Криптографические алгоритмы. Классификация криптографических алгоритмов. Симметричные алгоритмы шифрования. Асимметричные криптоалгоритмы.			
	3	Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Строгая аутентификация. Биометрическая аутентификация пользователя.		2	
	Практические работы			4	
	1	Изучение стандарта криптографической защиты AES (Advanced Encryption Standart).			
2	Изучение отечественных стандартов хэш-функции и цифровой подписи.				
Тема 2.4. Технологии защиты межсетевых обмена данными	Содержание		12	2	
	1	Обеспечение безопасности операционных систем. 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.			
	3	Основы технологии виртуальных защищенных сетей VPN. Концепция построения виртуальных защищенных сетей VPN. VPN-решения для построения защищенных сетей. Достоинства применения технологий VPN.			
	4	Защита на канальном и сеансовом уровнях. Протоколы формирования защищенных каналов на канальном уровне. Протоколы формирования защищенных каналов на сеансовом уровне. Защита беспроводных сетей.			
	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.			
	6	Инфраструктура защиты на прикладном уровне. Управление идентификацией и доступом. Организация защищенного удаленного доступа. Управление доступом по схеме однократного входа с авторизацией Single Sign-On. Протокол Kerberos. Инфраструктура управления открытыми ключами PKI			2

7	Анализ защищенности и обнаружение атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак.		2
8	Защита от вирусов. Методы управления средствами сетевой безопасности. Компьютерные вирусы и проблемы антивирусной защиты. Антивирусные программы и комплексы.		2
9	Построение системы антивирусной защиты корпоративной сети. Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности.		2
Практические работы		11	
1	Компоненты межсетевого экрана. Политика межсетевого экранирования		
2	Архитектура МЭ. Пример реализации политики МЭ.		
3	Применение МЭ на основе двудомного узла. Применение МЭ на основе фильтрующего маршрутизатора. Применение МЭ на основе экранирующего узла		
4	Применение технологии трансляции сетевых адресов.		
5	Задачи, решаемые VPN. Туннелирование в VPN. Уровни защищенных каналов. Защита данных на канальном уровне.		
6	Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне		
7	Организация VPN средствами СЗИ VipNet. Использование протокола IPSec для защиты сетей.		
8	Организация VPN средствами протокола SSL в Windows Server		
9	Сигнатурный анализ и обнаружение аномалий		
10	Обнаружение в реальном времени и отложенный анализ. Локальные и сетевые системы		
11	Распределенные системы обнаружения атак. Система обнаружения атак Snort.		
Самостоятельная работа		6	
1.	Составление доклада о критериях защиты информации.		
2.	Подготовка реферата по теме «Линейная структура защиты информации».		
3.	Схема «Классы защиты автоматизированных систем».		
4.	Схема «Нормативно-правовое регулирование защиты информации».		
5.	Схема «Источник несанкционированного доступа к информации».		
6.	Подготовка презентаций «Защита операционной системы Windows»		

	Настройка прав доступа.
	Оформление технической документации, правила оформления документов.
	Настройка аппаратного и программного обеспечения сети.
	Программная диагностика неисправностей
	Программная диагностика неисправностей
	Программная диагностика неисправностей
	Аппаратная диагностика неисправностей
	Аппаратная диагностика неисправностей
	Аппаратная диагностика неисправностей
	Поиск неисправностей технических средств
	Поиск неисправностей технических средств
	Поиск неисправностей технических средств
	Выполнение действий по устранению неисправностей
	Выполнение действий по устранению неисправностей
	Выполнение действий по устранению неисправностей
	Изучение утилиты Acronis
	Изучение утилиты Acronis
	Изучение утилиты Acronis
	Использование активного оборудования сети.
	Использование пассивного оборудования сети.
	Устранение паразитирующей нагрузки в сети.
	Заполнение технической документации.
	Построение физической карты локальной сети.
	Работа по созданию, редактированию, удалению пользователей в DOMAIN.
	Регламенты технических осмотров.
	Профилактические работы в объектах сетевой инфраструктуры.
	Мониторинг и анализ сети с помощью программных и аппаратных средств
	Структура системы управления, архитектура системы управления.

	Управление областями сети: ошибками, конфигурацией, доступом, производительностью,		
	Работа с протоколами SNMP; CMIP; TMN; LNMP; ANMP.		
	Отслеживание работы сети.		
	Работа с сервером, чтение логов, работа над ошибками		
	Работа с сервером.		
	Удаленное администрирование рабочих станций с сервера		
	Контроль доступа, сохранение целостности данных и журналирование.		
	Удаленное администрирование сервера с рабочих станций, программы для удаленного доступа.		
	Архитектура сети Интернет		
	Использование модели уровней		
	Примеры протоколов и сервисов прикладного уровня		
	Протокол управления передачей TCP - надёжная коммуникация		
	Протокол дейтаграмм пользователя UDP - коммуникация с малой нагрузкой		
	IPv4		
	Маршрутизация - как обрабатываются наши пакеты		
	Процесс маршрутизации: как узнаются маршруты		
	Адресация IPv4		
	Вычисление адресов		
	Канальный уровень - Доступ к среде передачи		
	Адресация при доступе к среде и формирование кадров		
	Физический уровень - коммуникация сигналов		
	Ethernet - коммуникации через локальную сеть		
	Кадр Ethernet		
	Хабы и свитчи		
	Протокол разрешения адресов ARP		
	Настройка устройств Cisco - Основы IOS		
ПП.03	Производственная практика	324	
	Анализ трафика сети		
	Анализ трафика сети		
	Анализ трафика сети		
	Работа с кабельными сканерами и тестерами		
	Работа с кабельными сканерами и тестерами		
	Работа с кабельными сканерами и тестерами		
	Работа со встроенными сканерами диагностики и управления.		
	Работа со встроенными сканерами диагностики и управления.		

	Работа со встроенными сканерами диагностики и управления.
	Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных
	Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных таблиц
	Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных
	Восстановление сети после сбоя.
	Восстановление сети после сбоя.
	Восстановление сети после сбоя.
	Создание плана восстановления сети
	Создание плана восстановления сети
	Создание плана восстановления сети
	Использование в работе контрольно
	Использование в работе контрольно
	Использование в работе контрольно

	Разработка функциональных схем элементов автоматизированной системы защиты
--	--

	информации	
	Разработка функциональных схем элементов автоматизированной системы защиты информации	
	Разработка функциональных схем элементов автоматизированной системы защиты информации	
	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование	
	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование	
	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование	
	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование	
	Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование	
	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации	
	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации	
	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации	
	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации	
	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации	
	Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации	
	Разработка политик безопасности и внедрение их в операционные системы	
	Разработка политик безопасности и внедрение их в операционные системы	
	Разработка политик безопасности и внедрение их в операционные системы	
	Разработка политик безопасности и внедрение их в операционные системы	
	Разработка политик безопасности и внедрение их в операционные системы	
	Разработка политик безопасности и внедрение их в операционные системы	
	Настройка IPSec и VPN. Настройка межсетевых экранов	
	Настройка IPSec и VPN. Настройка межсетевых экранов	

	Настройка IPSec и VPN. Настройка межсетевых экранов	
	Настройка IPSec и VPN. Настройка межсетевых экранов	
	Настройка IPSec и VPN. Настройка межсетевых экранов	
	Настройка IPSec и VPN. Настройка межсетевых экранов	
	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств	
	Настройка защиты беспроводных сетей с помощью систем шифрования	
	Настройка защиты беспроводных сетей с помощью систем шифрования	
	Настройка защиты беспроводных сетей с помощью систем шифрования	
	Настройка защиты беспроводных сетей с помощью систем шифрования	
	Настройка защиты беспроводных сетей с помощью систем шифрования	
	Настройка защиты беспроводных сетей с помощью систем шифрования	
	Архивация и восстановление ключей в Windows Server (PKI).	
	Архивация и восстановление ключей в Windows Server (PKI).	
	Архивация и восстановление ключей в Windows Server (PKI).	
	Архивация и восстановление ключей в Windows Server (PKI).	
	Архивация и восстановление ключей в Windows Server (PKI).	
	Установка и настройка системы обнаружения атак Snort.	
	Установка и настройка системы обнаружения атак Snort.	
	Установка и настройка системы обнаружения атак Snort.	
	Установка и настройка системы обнаружения атак Snort.	
	Установка и настройка системы обнаружения атак Snort.	
	Установка и настройка системы обнаружения атак Snort.	
	Установка и настройка системы обнаружения атак Snort.	
	Установка и настройка системы обнаружения атак Snort.	
	Всего	

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)

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к материально-техническому обеспечению

Реализация профессионального модуля предполагает наличие лабораторий эксплуатации объектов сетевой инфраструктуры и программно-аппаратной защиты объектов сетевой инфраструктуры, а также полигона технического контроля и диагностики сетевой инфраструктуры.

Лаборатория эксплуатации объектов сетевой инфраструктуры Оборудование лаборатории и рабочих мест мастерской:

- Оборудование лаборатории и рабочих мест лаборатории: 12 компьютеров ученика и 1 компьютер учителя;
- Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ-45, тестеры для кабеля);
- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности.

Оборудование и технологическое оснащение рабочих мест:

- Компьютер ученика (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО - CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)
- Компьютер учителя (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО - CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР).
- Сервер в лаборатории (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; Жесткий диск объемом не менее 1Тб; программное обеспечение: Windows Server 2003 или Windows Server 2008; лицензионные антивирусные программы; лицензионные программы восстановления данных.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением
- интерактивная доска
- проектор

Лаборатория программно-аппаратной защиты объектов сетевой инфраструктуры:

Оборудование мастерской и рабочих мест мастерской:

- Оборудование лаборатории и рабочих мест лаборатории: 12 компьютеров ученика и 1 компьютер учителя;
- Типовое активное оборудование: сетевые маршрутизаторы, сетевые коммутаторы, сетевые хранилища, сетевые модули и трансиверы, шасси и блоки питания, шлюзы VPN, принт-серверы, IP - камеры, медиа-конвертеры, сетевые адаптеры и карты, сетевые контроллеры, оборудование xDSL, аналоговые модемы, коммутационные панели, беспроводные маршрутизаторы, беспроводные принт-серверы, точки доступа WiFi, WiFi - адаптеры, Bluetooth - адаптеры, [KVM-коммутаторы](#), [KVM-адаптеры](#), [VoIP маршрутизаторы](#), [VoIP-адаптеры](#);
- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности.

Оборудование и технологическое оснащение рабочих мест:

- Компьютер ученика (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО - CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)
- Компьютер учителя (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; программное обеспечение: лицензионное ПО - CryptoAPI, операционные системы Windows, UNIX, MS Office, пакет САПР)
- Сервер в лаборатории (Аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 2 Гб; Жесткий диск объемом не менее 1Тб;

программное обеспечение: Windows Server 2003 или Windows Server 2008; лицензионные антивирусные программы; лицензионные программы восстановления данных.

Перечень программного обеспечения:

1. MS Windows 7
 2. MS Office 2007
 3. MS Windows 2003/2008
 4. Ethereal, разработчик-Gerald Combs (C)1998-2005, источник - <http://www.ethereal.com>, версия 0.10.11.
 5. InterNetView, разработчик-Evgeny Ilchenko, источник - <http://www.tsu.ru/~evgene/info/inv>, версия 2.0.
 6. Netcat, разработчик -WeldPond <weld@10pht.com>,
 7. Nmap, разработчик Copyright 2005 Insecure.Com, источник - <http://www.insecure.com>, версия 3.95.
 8. Snort, разработчик - Martin Roesch & The Snort Team. Copyright 1998-2005 Sourcefire Inc., et al., источник - <http://www.snort.org>, версия 2.4.3.
 9. VipNet Office, разработчик - ОАО Инфотекс, Москва, Россия, источник - <http://www.infotecs.ru>, версия 2.89 (Windows).
 10. VMware Workstation, разработчик - VMware Inc, источник - <http://www.vmware.com>, версия 4.0.0.
 11. WinPCap, источник - <http://winpcap.polito.it>.
 12. AdRem Netcrunch, источник - <http://www.adremsoft.com/netcrunch/>
- Nessus, источник - <http://www.nessus.org>

4.2. Информационное обеспечение обучения

Основные источники:

1. Виснадул, Б.Д. Основы компьютерных сетей: учебное пособие для учреждений СПО/ Б.Д.Виснадул, С.А.Лупин, С.В. Сидоров; под ред. Л.Г.Гагариной. - М.: ФОРУМ: Инфра- М, 2021.
2. Кузин, А.В. Компьютерные сети: учебное пособие для студ. учреждений СПО. - М.: Форум: ИНФРА-М, 2021.
3. Назаров, А.В. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений СПО.- М.: Академия, 2021.
4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов/В.Г.Олифер, Н.А.Олифер. - СПб.: Питер, 2020.
5. Таненбаум, Э. Компьютерные сети/Э.Таненбаум, Д.Уэзеролл. - СПб.: Питер, 2021.
6. Технологии разработки и создания компьютерных сетей на базе аппаратуры D-LINK: учебное пособие для вузов/ В. В.Барин, А. В.Благодаров, Е. А.Богданова, А. Н.Пылькин, Д. М.Скуднел. - М.: Горячая линия-Телеком, 2021.
7. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для СПО /А.В.Васильков, И.А.Васильков. - М.: ФОРУМ, 2021.
8. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учреждений СПО/ В.Я.Ищейнов, М.В.Мецатунян. - М.: Форум: ИНФРА-М, 2020.
9. Партыка, Т.Л. Информационная безопасность: учебное пособие для студ. учреждений СПО /Т.Л.Партыка, И.И.Попов. - М.: Форум, 2020.
10. Рябко, Б.Я. Основы современной криптографии и стеганографии / Б.Я.Рябко, А.Н.Фионов. - М.: Горячая линия-Телеком, 2020.
11. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие для вузов. - М.: Форум: Инфра-М, 2020.
12. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учреждений СПО/В.Ф.Шаньгин. - М.: ФОРУМ: ИНФРА-М, 2020.
13. Гольдштейн, Б.С. IP-телефония / Б.С.Гольдштейн, А.В.Пинчук, А.Л.Суховицкий. - СПб. БХВ-Петербург, 2021.
14. Гольдштейн Б. С. Call-центры и компьютерная телефония/Б.С.Гольдштейн, В.А.Фрейнкман. - СПб.: БХВ-Петербург, 2021.
15. Гольдштейн Б. С. Softswitch/ Б.С..Гольдштейн, А.Б.Гольдштейн. - СПб.: БХВ-Петербург, 2021.

Интернет-ресурсы:

1. CIT-Forum: Центр информационных технологий: материалы сайта [Электронный ресурс]. - Режим доступа: <http://citforum.ru/>, свободный.
2. Библиотека учебных курсов Microsoft [Электронный ресурс]. - Режим доступа: <http://msdn.microsoft.com/ru-ru/gg638594>, свободный.
3. Интернет-Университет информационных технологий. Библиотека учебных курсов [Электронный ресурс]. - Режим доступа: <http://old.intuit.ru>, свободный.
4. Сайт компании Cisco [Электронный ресурс]. - Режим доступа: <http://www.cisco.ru/>, свободный.
5. Сайт компании D-Link [Электронный ресурс]. - Режим доступа: <http://www.dlink.ru/>, свободный.
6. Небаев, И.А. Разработка единой компьютерной сети передачи данных на базе технологии Ethernet и протокола IP [Электронный ресурс]: учебное пособие к курсовому проектированию/Кафедра обработки и передачи данных СПбГУТ. - 2014. - Режим доступа: http://opds.sut.ru/wp-content/uploads/mu/kspd_project.pdf, свободный.
7. SecurityLab. Защита информации и информационная безопасность [Электронный ресурс]: информационный портал/ООО "Positive Technologies". - Режим доступа: <http://www.securitylab.ru>, свободный.
8. VoIPReview: информационный сайт [Электронный ресурс]. — Режим доступа: <http://voipreview.ru/>, свободный.
9. Атцик, А.А. IP-коммуникации в NGN [Электронный ресурс]: учебное пособие / А. А. Атцик, А. Б. Гольдштейн, В. В. Саморезов. - СПб. : СПбГУТ, 2015. — Режим доступа: http://libr.itut.ru/Jirbis2_spbgut/index.php?option=com_irbis&view=irbis&Itemid=308, свободный.
10. Гольдштейн, А.Б. IP-телефония [Электронный ресурс]: методические рекомендации к лабораторным работам/ А. Б. Гольдштейн, В. В. Саморезов. - СПб. : СПбГУТ, 2003.— Режим доступа: http://libr.itut.ru/Jirbis2_spbgut/index.php?option=com_irbis&view=irbis&Itemid=308, свободный.
11. Гольдштейн, Б.С. Протоколы IP-телефонии: RTP, RTCP [Электронный ресурс] : учебное пособие / Б. С. Гольдштейн, В. Ю. Гойхман, Ю. В. Столповская". - СПб. : СПбГУТ, 2014. — Режим доступа: http://libr.itut.ru/Jirbis2_spbgut/index.php?option=com_irbis&view=irbis&Itemid=308, свободный.
12. Некоторые аспекты технологий IP-телефонии [Электронный ресурс]. — Режим доступа: <http://www.ixbt.com/comm/ip-aspects.html>, свободный.

4.3. Общие требования к организации образовательного процесса

Программа профессионального модуля обеспечивается учебно-методической документацией по всем разделам междисциплинарного курса.

Внеаудиторная работа сопровождается методическим обеспечением и обоснованием времени, затрачиваемого на ее выполнение.

Реализация программы профессионального модуля обеспечивается доступом каждого обучающегося к базам данных и библиотечным фондам, формируемым по полному перечню разделов модуля. Во время самостоятельной подготовки обучающиеся обеспечиваются доступом к сети Интернет.

Материально-техническая база, перечисленная в п. 4.1, обеспечивает проведение всех видов практических занятий, практики. Материально-техническая база должна соответствовать действующим санитарным и противопожарным нормам.

Консультации предусматриваются в объеме 100 часов на учебную группу на каждый учебный год, в том числе в период реализации среднего (полного) общего образования для лиц, обучающихся на базе основного общего образования. Формы проведения консультаций: групповые, индивидуальные, письменные, устные.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): реализация программы профессионального модуля должна обеспечиваться педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемого модуля.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального модуля в рамках производственной практики, эти преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

Инженерно-педагогический состав: высшее образование, соответствующее профилю преподаваемого модуля.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения практических и лабораторных занятий, тестирования.

<i>Результаты (освоенные профессиональные компетенции)</i>	<i>Основные показатели оценки результата</i>	<i>Формы и методы контроля и оценки</i>
Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей	<ul style="list-style-type: none"> – точность и скорость настройки сети; – качество рекомендаций по повышению работоспособности сети; – выбор технологического оборудования для настройки сети; – расчет времени для настройки сети; – точность и грамотность оформления технологической документации. 	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы <ul style="list-style-type: none"> - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики
Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях	<ul style="list-style-type: none"> – точность и скорость настройки сети; – качество анализа свойств сети, исходя из ее служебного назначения; – качество рекомендаций по повышению технологичности сети; – точность и грамотность оформления технологической документации. 	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы <ul style="list-style-type: none"> - на практических занятиях, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики
Осуществлять эксплуатацию сетевых конфигураций	<ul style="list-style-type: none"> – точность и скорость настройки сети; – качество анализа и рациональность выбора сетевых конфигураций; – выбор способов настройки и технологически грамотное назначение технологической базы 	Экспертная оценка результатов Деятельности обучающихся в процессе освоения образовательной программы <ul style="list-style-type: none"> - на практических занятиях, -при выполнении определенных видов работ производственной практики, - зачет по разделу практики
Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и	<ul style="list-style-type: none"> – выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических 	Экспертная оценка результатов Деятельности обучающихся в процессе освоения образовательной программы <ul style="list-style-type: none"> - на практических занятиях,

резервное копирование информации	процессов	-при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, - зачет по разделу практики
Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования	– выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, - зачет по разделу практики
Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	– выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики Междисциплинарный экзамен

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.

<i>Результаты (освоенные профессиональные компетенции)</i>	<i>Основные показатели оценки результата</i>	<i>Формы и методы контроля и оценки</i>
Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	1) Формулировка области и объектов профессиональной деятельности техника-программиста по разработке и адаптации ПО в соответствии с ФГОС по специальности 230701 Прикладная информатика (по отраслям); 2) участие в профессиональных конкурсах, конференциях, проектах, выставках, фестивалях, олимпиадах	- <i>оценка на экзамене по модулю</i> - <i>оценка профессионального портфолио студента на экзамене по модулю</i>
Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	1) четкое выполнение должностных обязанностей в рамках конкретного проекта 2) дана адекватная оценка эффективности и качества выбранных методов решения профессиональных задач	- <i>интерпретация результатов наблюдения на производственной практике;</i> - <i>оценка анализа эффективности методов решения профессиональных задач на производственной практике</i>

Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях	-верность принятия решения в смоделированной нестандартной ситуации по разработке и адаптации ПО с оценкой возможных рисков при их реализации;	<i>Накопительная оценка за решения смоделированных нестандартных ситуации на учебной практике</i>
Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития	отобранная на основе анализа и оценки информация позволяет ставить и решать профессиональные задачи и задачи профессионального и личностного развития	<i>Накопительная оценка за представленную информацию на учебной практике</i>
Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности	для разработки и адаптации ПО использованы современ-ные информационно-коммуникационные технологии	<i>интерпретация результата наблюдения за деятельностью на производственной практике</i>
Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.	- эффективность взаимодействия с коллегами, клиентами при разработке технического задания проекта	<i>интерпретация результата наблюдения за деятельностью студента на производственной практике</i>
Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.	при обеспечении проектной деятельности: - верно поставлены цели и осуществлена мотивация подчиненных, - эффективно организована работа с подчиненными, - верно выбраны методы контроля за качеством проведения проектных операций;	<i>интерпретация результата наблюдения за деятельностью студента на производственной практике</i>
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	1) верно определены задачи профессионального и личностного развития; 2) план самообразования обоснован задачами профессионального и личностного развития и включает мероприятия по повышению квалификации;	<i>оценка плана самообразования на учебной практике</i>
Быть готовым к смене технологий в профессиональной деятельности.	- проектная деятельность организована с использованием новых отраслевых технологий	<i>интерпретация результата наблюдения за деятельностью студента на производственной практике</i>
Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).	-эффективность использования полученных профессиональных знаний для исполнения воинской обязанности	<i>экспертная оценка на военных сборах</i>