Приложение II.3

к программе СПО 11.02.15 «Инфокоммуникационные сети и системы связи»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

2023

Составитель:

Кислицин Никита Алексеевич, преподаватель ГБПОУ УКРТБ

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

наименование профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему профессиональные компетенции и общие компетенции:

Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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	Пользоваться профессиональной документацией на государственном и иностранных языках

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи
ПК 3.1.	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности
ПК 3.2.	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи
ПК 3.3.	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования

В ходе освоения профессионального модуля учитывается движение к достижению личностных результатов обучающимися ЛР 17,18.

В результате освоения профессионального модуля студент должен:

Иметь практический опыт в	- анализировать сетевую инфраструктуру; - выявлять угрозы и уязвимости в сетевой инфраструктуре, - разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи, - осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи - использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.
уметь	- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; - проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей; - определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи; - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты - выполнять тестирование систем с целью определения уровня защищенности, - определять оптимальные способы обеспечения информационной безопасности; - проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях, - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации; - разрабатывать политику безопасности сетевых элементов и логических сетей; - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи; - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; - защищать базы данных при помощи специализированных программных продуктов; - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.
знать	- принципы построения информационно-коммуникационных сетей; - международные стандарты информационной безопасности для проводных и беспроводных сетей; - нормативно - правовые и законодательные акты в области информационной безопасности; - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия; - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

	- способы и методы обнаружения средств съёма информации в радиоканале; - классификацию угроз сетевой безопасности; - характерные особенности сетевых атак; - возможные способы несанкционированного доступа к системам связи, - правила проведения возможных проверок согласно нормативным документам ФСТЭК; - этапы определения конфиденциальности документов объекта защиты; назначение, классификацию и принципы работы специализированного оборудования; - методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP. WPA и WPA 2; - методы и средства защиты информации в телекоммуникациях от вредоносных программ; - технологии применения программных продуктов; - возможные способы, места установки и настройки программных продуктов, - методы и способы защиты информации, передаваемой по кабельным направляющим системам; конфигурации защищаемых сетей; - алгоритмы работы тестовых программ; - средства защиты различных операционных систем и среды передачи информации; - способы и методы шифрования (кодирование и декодирование) информации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов – 228 часа, в том числе:

- 24 часов вариативной части, направленных на усиление обязательной части программы профессионального модуля.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Суммарный объем нагрузки, час	Объем профессионального модуля, час						
			Обучение по МДК				Практика		Промежуточная аттестация
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Самостоятельная работа	Учебная, часов	Производственная (по профилю специальности), часов	
1	2	3	4	5	6	7	8	9	10
ПК 3.1, ПК 3.2, ПК 3.3	**Раздел 1.** Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	**120**	**120**	**62**		**12**			**4**
ПК 3.1, ПК 3.2, ПК 3.3	**Учебная практика**	**36**					**36**		
ПК 3.1, ПК 3.2, ПК 3.3	**Производственная практика (по профилю специальности)**, часов	**72**						**72**	
	Промежуточная аттестация (экзамен (квалификационный))	**7**							
	Всего:	**228**	**120**	**62**			**36**	**72**	**4**

*Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

2.2. Тематический план и содержание профессионального модуля (ПМ)

VI семестр

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся , курсовая работ (проект)		Объем часов
1	**2**		**3**
Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи			**40**
МДК 03.01 Защита информации в инфокоммуникационных системах и сетях связи			**40**
Тема 1.1. Основы безопасности информационных технологий	**Содержание**		**40**
	1	Вводная лекция.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 66-72	
	2	Основы информационной безопасности	2
		Домашнее задание: чтение и анализ литературы [1] стр. 73-76	
	3	Проблемы безопасности ОС.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 77-80	
	4	Технологии: идентификации, аутентификации, авторизации.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 81-82	
	5	Архитектура подсистемы защиты.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 83-86	
	6	Разграничение доступа.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 87-90	
	7	Файловая система Windows.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 91-96	
	8	АПМДЗ.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 97-100	
	9	RAID.	2
		Домашнее задание: чтение и анализ литературы [1] стр.110-112	
	Практические занятия		18

	1	Обзор VMware Workstation Pro.	
	2	Установка виртуальной машины (Windows 10).	
	3	Редактор реестра в Windows.	
	4	Редактор локальной групповой политики в Windows.	
	5	Службы в Windows.	
	6	Управление дисками в Windows.	
	7	Диспетчер задач в Windows.	
	8	Просмотр событий в Windows.	
	9	Планировщик заданий в Windows.	
	Самостоятельная работа		4
	Подготовить выступление на тему «Уязвимости в операционной системе Windows».		
	VII семестр		**80**
Тема 1.2 Обеспечение безопасности информационных технологий	**Содержание**		**36**
	1	Введение в Active Directory.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 123-125	
	2	Канальный уровень.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 126-129	
	3	Защита на канальном уровень.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 130-131	
	4	Протокол DHCP.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 132-135	
	Практические занятия		20
	10	Установка виртуальной машины (Windows Server 2022).	
	11	Обзор Windows Admin Center.	
	12	Развертывание роли DNS в Windows Server.	
	13	Развертывание роли DHCP в Windows Server.	
	14	Развертывание основного контролера домена Active Directory в Windows Server.	
	15	Развертывание дополнительного контроллера домена в существующий домен Active Directory в Windows Server.	
	16	Обзор управлений пользовательскими и служебными учетными записями в Windows Server.	
	17	Обзор введения пользователя в домен.	
	18	Развертывание инфраструктуры групповых политик в Windows Server.	
	19	Развертывание роли Web Server IIS в Windows Server.	
	Самостоятельная работа		8

	Подготовить выступление на тему «Уязвимости в операционной системе Windows server».		
Тема 1.3. Обеспечение безопасности стандартными средствами защиты	**Содержание**		**24**
	1	Защита на сетевом уровне.	2
		Домашнее задание: чтение и анализ литературы [3] стр. 123-125	
	2	Протоколы IPv4 и IPv6.	2
		Домашнее задание: чтение и анализ литературы [4] стр. 123-125	
	3	Транспортный уровень.	2
		Домашнее задание: чтение и анализ литературы [2] стр. 123-125	
	4	Защита на транспортном уровне.	2
		Домашнее задание: чтение и анализ литературы [3] стр. 123-125	
	Практические занятия		**16**
	20	Монитор стабильности системы в Windows.	
	21	Системного монитора в Windows.	
	22	Монитор ресурсов в Windows.	
	23	Брандмауэр в Windows.	
	24	Установка виртуальной машины (Windows Server 2022).	
	25	Обзор Windows Admin Center.	
	26	Развертывание роли DNS в Windows Server.	
	27	Развертывание роли DHCP в Windows Server.	
Тема 1.4. Криптографическая защита информации	**Содержание**		**16**
	1	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных	2
		Домашнее задание: чтение и анализ литературы [6] стр. 64-66	
	2	Симметричные криптосистемы. Ассимметричные криптосистемы	2
		Домашнее задание: составить план конспекта лекции	
	3	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	2
		Домашнее задание: чтение и анализ литературы [6] стр. 66-72	
	4	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи.	2
		Домашнее задание: чтение и анализ литературы [6] стр. 72-75	
	Практические занятия		**8**
	28	Бинарная арифметика. Модульная арифметика	
	29	Применение методов шифрования перестановкой	

	30	Применение методов шифрования заменой	
	31	Применение методов шифрования многоалфавитной замены	
Промежуточная аттестация (экзамен)			4
Учебная практика **Виды работ**			**36**
1	Подключение, установка стенда, виртуальной машины ТМ. Подключение, установка драйверов, настройка виртуальной машины агента		6
2	Подключение, настройка DLP системы Infowatch Настройка агентских политик на ARM Настройка политик на Device Monitor Настройка политик на Traffic Monitor		6
3	Выполнение заданий, настройка агентских политик на ARM		6
4	Выполнение заданий, настройка политик на Device Monitor		6
5	Выполнение заданий, настройка политик на Traffic Monitor		6
6	Оформление отчета. Защита отчета по учебной практике		6
Производственная практика(по профилю специальности) **Виды работ**			**72**
1	Участие в создании комплексной системы защиты на предприятии.		12
2	Применение программно-аппаратных средств защиты информации на предприятии		12
3	Применение инженерно-технических средств защиты информации на предприятии		18
4	Применение криптографических средств защиты информации на предприятии.		18
5	Оформление отчета. Защита отчета по производственной практике		6
Промежуточная аттестация (экзамен (квалификационный))			**7**
Всего:			**228**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Кабинет «Компьютерного моделирования», лаборатории «Информационной безопасности телекоммуникационных систем», «Телекоммуникационных систем», оснащенные в соответствии с программой по специальности 11.02.15, а именно:

- компьютеры в комплекте (системный блок, монитор, клавиатура, манипулятор «мышь») или ноутбуки (моноблоки),
- локальная сеть с выходом в Интернет,
- комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном)
- программное обеспечение

Оборудование лаборатории:

- автоматизированные рабочие места обучающихся (ПК с доступом в интернет и программным обеспечением общего и профессионального назначения (для расчета и проектирования узлов электро- и радиосвязи);
- автоматизированное рабочее место преподавателя (ПК с доступом в интернет и программным обеспечением общего и профессионального назначения (для расчета и проектирования узлов электро- и радиосвязи);
- доска;
- комплект учебно-наглядных пособий и плакатов;
- мультимедийное оборудование;
- управляемый коммутатор;
- управляемый межсетевой экран-маршрутизатор;
- устройства преобразования оптических-, электро- и радиосигналов (конвертеры, точки доступа WLAN, мультиплексоры);
- комплекты пассивных элементов (расходных материалов) для подключения абонентских терминалов и выполнения кроссировки;
- набор инструментов для выполнения кроссировочных работ.

3.2. Информационное обеспечение обучения

Основные источники:

1. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие/ Фороузан Б.А.; пер. с англ. Под ред.А.Н. Берлина. - М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2020.-784с.:ил.,табл.-(Основы информационных технологий).
2. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи/ Под ред. доктора техн. Наук, профессора О.Б. Макаревича. – М.: Горячая линия – Телеком, 2019. -360с.: ил.
3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства –М.: ДМК Пресс, 2016. – 544с.:ил.
4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2021.-272с.:ил.
5. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2019.-528с.- (Профессиональное образование)
6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для вузов -5-е изд., перераб. и доп. – М.: - Горячая линия – Телеком, 2020. – 616с:ил.
7.Романов О.А. Организационное обеспечение информационной безопасности: учебник для студентов высш. учеб. заведений –М.: Издательский центр «Академия», 2020. – 192с.
8. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябов Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2021. – 363 с.
9. InfoWatch Traffic Monitor Руководство пользователя – М.: ЗАО "ИнфоВотч", 2022. – 178 с.: ил..

Интернет ресурсы:

1. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http:// www.znanium.com/ (2023).
2. http://www.fstec.ru сайт ФСТЭК РФ
3. http://www.ancad.ru сайт компании АНКАД
4. https://www.cryptopro.ru/ сайт компании КриптоПро
5. https://infotecs.ru/ сайт ОАО «ИнфоТеКС»
6. Центр оказания образовательных услуг и подготовки специалистов в области информационной безопасности и эксплуатации средств защиты информации ViPNet. [Электронный ресурс] – режим доступа: https://edu.infotecs.ru/learning/ (2023)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ПО РАЗДЕЛАМ)

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
Раздел 1 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.	тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

	Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- разбивает поставленную цель на задачи, подбирая из числа известных технологии (элементы технологий), позволяющие решить каждую из задач; - выбирает способ (технологию) решения задачи в соответствии с заданными условиями и имеющимися ресурсами;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- формулирует вопросы, нацеленные на получение недостающей информации; - характеризует произвольно заданный источник информации в соответствии с задачей информационного поиска; - извлекает информацию по двум и более основаниям из одного или нескольких источников и систематизирует ее в самостоятельно определенной в соответствии с задачей информационного поиска структуре; - задает критерии для сравнительного анализа информации в соответствии с поставленной задачей деятельности; - делает вывод о применимости общей закономерности в конкретных условиях;	
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	- анализирует /формулирует запрос на внутренние ресурсы (знания, умения, навыки, способы деятельности, ценности, установки, свойства психики) для решения профессиональной задачи;	

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде	- принимает и фиксирует решение по всем вопросам для группового обсуждения; - при групповом обсуждении: развивает и дополняет идеи других (разрабатывает чужую идею); - использует средства наглядности или невербальные средства коммуникации; - запрашивает мнение партнера по диалогу;	
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	- извлекает из устной речи (монолог, диалог, дискуссия) фактическую и оценочную информацию, определяя основную тему, звучавшие предположения, аргументы, доказательства, выводы, оценки; - создает продукт письменной коммуникации сложной структуры, содержащий сопоставление позиций и \ или аргументацию за и против предъявленной для обсуждения позиции;	
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- способность ориентироваться в основных методах и системах обеспечения техносферной безопасности, обоснованно выбирать устройства, системы и методы защиты человека и природной среды от опасностей;	
ОК 8. Использовать средства физической культуры для	- овладение технологиями современных оздоровительных систем физического воспитания, обогащение индивидуального	

сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	опыта занятий специально-прикладными физическими упражнениями и базовыми видами спорта;	
ОК 9. Пользоваться профессиональной документацией на государственном и иностранных языках	- осуществление межкультурной коммуникации в сфере основной профессиональной деятельности;	

Приложение 1
Обязательное

КОНКРЕТИЗАЦИЯ ДОСТИЖЕНИЯ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ

Личностные результаты	Содержание урока (тема, тип урока, воспитательные задачи)	Способ организации деятельности	Продукт деятельности	Оценка процесса формирования ЛР
ЛР 17 Осуществляющий техническую эксплуатацию инфокоммуникационных систем ЛР 18 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи	Тема День специалиста ИТ (4 ч.) Тип урока: комплексного применения знаний и способов деятельности – деловая игра Воспитательная задача: - закрепление и углубление имеющихся навыков и умений; - развитие ответственного отношения к организации и ходу продуктивной деятельности при выполнении проектных работ	Викторина по информационным технологиям с использование электронных средств и проектов. Состоит из 2 частей, теоретическая игра Quiz и защита проектов по ИТ	Выступление и проекты по ИТ студентов, а так же комплексное закрепление и применение знаний.	- эмоциональное отношение к своей будущей профессии - умение работать и выполнять требования трудовой дисциплины