**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПб ГУТ))) **Документ подписан простой электронной подписью**

Сертификат: 009b47d8b89b08d0f6
Владелец: Киричек Руслан Валентинович
Действителен с 13.02.2023 по 12.02.2028

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
_____ 2025 г.

Регистрационный № 11.09.25/128

РАБОЧАЯ ПРОГРАММА

ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

(наименование вида практики)

по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)

квалификация
техник по защите информации

Санкт-Петербург
2025

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утверждённым ректором ФГБОУ ВО «Санкт Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 28 марта 2025 г., протокол № 3.

Составитель:
Преподаватель _____ Н.В. Кривоносова
(подпись)

СОГЛАСОВАНО
Главный специалист НТБ УИОР _____ Р.Х. Ахтреева
(подпись)

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 9 (Информационной безопасности телекоммуникационных систем)
12 февраля 2025 г., протокол № 6

Председатель предметной (цикловой) комиссии: _____ Н.В. Кривоносова
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
19 февраля 2025 г., протокол № 4

Заместитель директора по учебной работе колледжа СПб ГУТ _____ Н.В. Калинина
(подпись)

СОГЛАСОВАНО

Директор колледжа СПб ГУТ _____ Т.Н. Сиротская
(подпись)

СОГЛАСОВАНО
Директор департамента ОКОД _____ С.И. Ивасишин
(подпись)

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ

Практическая подготовка – форма организации образовательной деятельности при освоении образовательной программы в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, в части освоения основных видов деятельности:

- Эксплуатация информационно-телекоммуникационных систем и сетей;
- Защита информации в информационно-телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты;
- Защита информации в информационно-коммуникационных системах и сетях с использованием технических средств защиты;
- Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»

Область профессиональной деятельности: 06 Связь, информационные и коммуникационные технологии, 12 обеспечение безопасности.

Практическая подготовка направлена на формирование у обучающихся общих и профессиональных компетенций, освоение современных производственных процессов, адаптация обучающихся к конкретным условиям деятельности организаций различных организационно-правовых форм, приобретение практического опыта в рамках профессиональных модулей по каждому из видов профессиональной деятельности предусмотренных по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Образовательная деятельность в форме практической подготовки организуется при реализации программ учебных практик (УП), производственных практик (ПП), преддипломных практик (ПДП), а также компонентов рабочих программ учебных дисциплин (профессиональных модулей) общепрофессионального и профессионального циклов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ

Результатом освоения рабочей программы практической подготовки в форме учебной или производственной практики (по профилю специальности) является сформированность у обучающихся общих и профессиональных компетенций, приобретение практического опыта в рамках профессиональных модулей по каждому из видов деятельности предусмотренных по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Код	Наименование результата обучения по специальности
ПК1.1.	Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей.
ПК 1.2.	Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно – телекоммуникационных систем и сетей.
ПК 1.3.	Проводить техническое обслуживание оборудования информационно – телекоммуникационных систем и сетей
ПК 1.4.	Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях
ПК 2.3.	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях.
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно – телекоммуникационных систем и сетей
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета

Код	Наименование результата обучения по специальности
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе
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 российских духовно-нравственных 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 иностранном языках

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ

3.1. Объём и виды учебной работы

Коды профессиональных компетенций	Наименования профессионального модуля (междисциплинарного курса)	Объём часов	Форма практической подготовки
ПК 1.1-ПК 1.4	ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей	180	ПП
	МДК.01.01.Приемо-передающие устройства, линейные сооружения связи и источники электропитания	36	УП
		80	ЛПЗ
	МДК.01.02.Телекоммуникационные системы и сети	72	УП
		120	ЛПЗ
	МДК.01.03. Электрорадиоизмерения и метрология	26	ЛПЗ
ПК 2.1-ПК 2.3	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе, криптографических средств защиты	180	ПП
	МДК.02.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	72	УП
		96	ЛПЗ
	МДК.02.02.Криптографическая защита информации	36	УП
		44	ЛПЗ
ПК 3.1-ПК 3.4	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	180	ПП
		108	УП
	МДК.03.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	100	ЛПЗ
	МДК.03.02.Физическая защита линий связи информационно-телекоммуникационных систем и сетей	70	ЛПЗ
ПК 4.1-4.4	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (Оператор электронно-вычислительных и вычислительных машин)	72	ПП
		72	УП
		34	ЛПЗ
	Всего часов	1578	

3.2. Тематический план и содержание

3.2.1. Содержание практической подготовки по **ПМ.01.Эксплуатация информационно-телекоммуникационных систем и сетей**

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов
Раздел 1. Приемо-передающие устройства, линейные сооружения связи и источники электропитания			
МДК.01.01. Приемо-передающие устройства, линейные сооружения связи и источники электропитания			
Тема 1.1. Линии связи	Содержание учебного материала		
	Лабораторные работы		
	1	Занятие 24. Разделка кабелей типа ПВ	34
	2	Занятие 25. Разделка кабелей типа ТПП	
	3	Занятие 26. Разделка кабелей типа СТС	
	4	Занятие 27. Симметричные кабели	
	5	Занятие 28. Коаксиальные кабели	
	6	Занятие 29. Волоконно-оптические линии связи	
	7	Занятие 30. Монтаж кабеля ТПП	
	8	Занятие 31. Монтаж кабеля МКС	
	9	Занятие 32. Монтаж кабеля ЗКП	
	10	Занятие 33. Монтаж КРТП-10, БМ	
	11	Занятие 34. Монтаж МТОК	
	12	Занятие 35. Измерение электрических характеристик симметричных кабелей	
	13	Занятие 36. Взаимное влияние в оптических кабелях.	
	14	Занятие 37. Причины взаимных влияний между цепями воздушных и кабельных линия связи	
	15	Занятие 38. Причины взаимных влияний между оптическими волокнами	
	16	Занятие 39. Исследование элементов защиты от внешних влияний	
	17	Занятие 40. Измерения при защите кабеля от коррозии	
Тема 1.2. Источники питания	Содержание учебного материала		
	Практические занятия		
	1	Занятие 5. Расчет параметров аккумуляторных батарей	4
	2	Занятие 6. Изучение аккумуляторов	
	Лабораторные работы		

	18	Занятие 7. Исследование управляемого выпрямителя на тиристорах	8
	19	Занятие 8. Исследование схем простейшего выпрямления трехфазного переменного тока	
	20	Занятие 9. Исследование параметров сглаживающих фильтров	
	21	Занятие 10. Исследование свойств параметрического стабилизатора напряжения	
Тема 1.3. Приемо-передающие устройства	Содержание учебного материала		
	Лабораторные работы		
	1	Занятие 18. Исследование влияния дестабилизирующих факторов на работу автогенератора	34
	2	Занятие 19. Исследование генератора, управляемого напряжением, используемого в синтезаторах частот	
	3	Занятие 20. Исследование умножителя частоты	
	4	Занятие 21. Исследование амплитудного модулятора	
	5	Занятие 22. Исследование частотного модулятора	
	6	Занятие 23. Регулировка усиления	
	7	Занятие 24. Настройки радиоприемников	
	8	Занятие 25. Регулировка полосы пропускания	
	9	Занятие 26. Устройства индикации РПМУ	
	10	Занятие 27. Назначение, параметры и принцип работы схем автоматической регулировки усиления	
	11	Занятие 28. Принцип автоматической подстройки частоты в радиоприемных устройствах	
	12	Занятие 29. Способы регулировки полосы пропускания приёмника	
	13	Занятие 30. Исследование резонансного усилителя радиочастоты	
	14	Занятие 31. Исследование преобразователя частоты с отдельным гетеродином	
	15	Занятие 32. Исследование усилителя промежуточной частоты	
	16	Занятие 33. Исследование отдельных функциональных блоков систем радиосвязи	
	17	Занятие 34. Исследование отдельных функциональных блоков систем радиосвязи	
УП.01.Учебная практика МДК.01.01. Приемо-передающие устройства, линейные сооружения связи и источники электропитания	Виды работ		
	1	Монтаж кабелей НЧ и ВЧ различными технологиями	36
	2	Монтаж оконечных устройств, применяемых на местных телефонных сетях, магистральных и зоновых линиях связи для электрических и оптических кабелей	
	3	Контроль качества монтажа с применением измерительных приборов постоянного тока	
	4	Определение вида и места повреждения кабельной линии связи с помощью приборов переменного тока (рефлектометров)	

	5	Монтаж оптических кабелей/ Проверка качества монтажа оптических волокон с помощью рефлектометров и измерителей оптической мощности	
	6	Разделка кабелей с «витой парой» для включения в коннекторы соответствующей емкости	
Раздел 2. Телекоммуникационные системы и сети			
МДК.01.02. Телекоммуникационные системы и сети			
Тема 2.1. Построение телекоммуникационных систем и сетей	Содержание учебного материала		
	Практические занятия		
	1	Занятие 11. Изучение принципов частотного разделения каналов (ЧРК).	8
	2	Занятие 12. Построение и система нумерации в телефонной сети связи.	
	3	Занятие 13. Расчет частот ГО цифровой системы передачи	
	4	Занятие 14. Формирование линейных кодов в цифровых системах передачи	
	Лабораторные работы		
	1	Занятие 15. Исследования спектра сигналов с импульсной модуляцией	14
	2	Занятие 16. Исследование принципа работы канала с ВРК	
	3	Занятие 17. Нелинейные кодеры взвешивающего типа	
	4	Занятие 18. Нелинейные декодеры взвешивающего типа	
	5	Занятие 19. Приемник сигналов цикловой синхронизации	
	6	Занятие 20. Преобразователь кода передачи	
	7	Занятие 21. Преобразователь кода приема	
Тема 2.2. Системы радиосвязи	Содержание учебного материала		
	Практические занятия		
	5	Занятие 30. Выбор кластера и расчет числа сот	8
	6	Занятие 31. Расчет основных параметров сетей подвижной связи	
	7	Занятие 32. Изучение принципа организации каналов СПС	
	8	Занятие 33. Кодирование речи в стандартах СПС	
Тема 2.3. Монтаж и эксплуатация телекоммуникационных систем и сетей	Содержание учебного материала		
	Лабораторные работы		
	8	Занятие 46. Измерение параметров каналов ТЧ анализатором телефонных каналов	50
	9	Занятие 47. Разработка проектов с помощью КПО-110 на МП ОГМ-30	
	10	Занятие 48. Организация локального и удаленного доступа в МП «Супертел»	
	11	Занятие 49. Измерение параметров групповых цифровых трактов	
	12	Занятие 50. Мониторинг оборудования	

	13	Занятие 51. Организация локального и удаленного конфигурирования оборудования	
	14	Занятие 52. Конфигурирование мультиплексора	
	15	Занятие 53. Конфигурирование источников синхронизации сетевого элемента мультиплексора	
	16	Занятие 54. Конфигурирование и резервирование трактов мультиплексора	
	17	Занятие 55. Анализ систем SDH при помощи анализатора NGSDH	
	18	Занятие 56. Изучение оборудования	
	19	Занятие 57. Организация локального и удаленного конфигурирования оборудования	
	20	Занятие 58. Изучение оборудования	
	21	Занятие 59. Инсталляция, конфигурирование и мониторинг оборудования	
	22	Занятие 60. Виды и назначение информационных и аварийных сигналов	
	23	Занятие 61. Просмотр и анализ аварийных сообщений	
	24	Занятие 62. Алгоритм поиска и устранения неисправностей	
	25	Занятие 63. Инсталляция, конфигурирование и мониторинг оборудования	
	26	Занятие 64. Виды и назначение информационных и аварийных сигналов	
	27	Занятие 65. Просмотр и анализ аварийных сообщений	
	28	Занятие 66. Алгоритм поиска и устранения неисправностей	
	29	Занятие 67. Инсталляция, конфигурирование и мониторинг оборудования	
	30	Занятие 68. Виды и назначение информационных и аварийных сигналов	
	31	Занятие 69. Просмотр и анализ аварийных сообщений	
	32	Занятие 70. Алгоритм поиска и устранения неисправностей	
	Практические занятия		
	6	Занятие 71. Мультиплексирование цифровых потоков	
	7	Занятие 72. Расчет основных параметров цифровых систем передачи	
	8	Занятие 73. Формирование линейных кодов абонентских линий	10
	9	Занятие 74. Формирование линейных кодов ВОСП	
	10	Занятие 75. Формирование модулей STM-N	
Курсовой проект Проект волоконно-оптической линии передачи сегмента транспортной сети на заданном участке	Обязательные аудиторные учебные занятия по курсовому проекту		
	1	Разработка схемы организации связи.	
	2	Выбор топологии сети.	
	3	Выбор типа оборудования.	30
	4	Выбор типа и конструкции оптического кабеля.	
	5	Расчет основных параметров оптического линейного тракта.	

	6	Расчет показателей надежности.	
УП.01.Учебная практика МДК.01.02. Телекоммуникационные системы и сети	Виды работ		
	1	Настройка оборудования транспортной сети мультиплексоров вода/вывода.	72
	2	Настройка оборудования транспортной сети терминальных мультиплексоров.	
	3	Настройка оборудования транспортной сети регенераторов.	
	4	Настройка оборудования транспортной сети кросконнекторов.	
	5	Настройка оборудования синхронизации транспортной сети.	
	6	Настройка оборудования абонентского доступа станционной части.	
	7	Настройка оборудования абонентского доступа ADSL2+.	
	8	Настройка оборудования абонентского доступа DSLAM.	
	9	Диагностика работы оборудования абонентского доступа станционной части.	
	10	Диагностика работы оборудования абонентского доступа ADSL2+.	
	11	Диагностика работы оборудования абонентского доступа DSLAM.	
	12	Настройка аппаратных IP-телефонов.	
	13	Настройка программных IP-телефонов.	
	14	Диагностика работы аппаратных IP-телефонов.	
	15	Диагностика работы программных IP-телефонов.	
	16	Подсоединение абонентского устройства к мультисервисной сети.	
	17	Диагностика работы абонентского устройства в мультисервисной сети.	
	18	Настройка и диагностика работы беспроводной сети.	
Раздел 3. Электрорадиоизмерения и метрология			
МДК.01.03. Электрорадиоизмерения и метрология			
Тема 3.1. Основы метрологии	Содержание учебного материала		
	Практические занятия		
	1	Занятие 7. Физические величины и их единицы	2
	Лабораторные работы		
	1	Занятие 8. Технические средства для измерений	4
	2	Занятие 9. Измерение физической величины	
Тема 3.2. Измерительные приборы	Содержание учебного материала		
	Лабораторные работы		
	3	Занятие 12. Аналоговые и цифровые измерительные приборы	4
	4	Занятие 13. Измерение электрического сигнала аналоговыми и цифровыми приборами	

Тема 3.4. Методы и средства измерения параметров сигналов	Содержание учебного материала		
	Лабораторные работы		
	5	Занятие 18. Измерение силы тока, напряжения, мощности	12
	6	Занятие 19. Изучение работы электронного осциллографа	
	7	Занятие 20. Измерение параметров электрического сигнала с помощью электронного осциллографа	
	8	Занятие 21. Измерение частоты и временного периода цифровым частотомером и электронным осциллографом	
	9	Занятие 22. Измерение фазового сдвига	
	10	Занятие 23. Измерение коэффициента амплитудной модуляции	
Тема 3.5. Методы и средства измерения параметров компонентов радиотехнических цепей	Содержание учебного материала		
	Лабораторные работы		
	11	Занятие 25. Измерение электрического сопротивления	4
	12	Занятие 26. Измерение амплитудно-частотных характеристик и нелинейных искажений	
ПП.01.Производственная практика (по профилю специальности)	Виды работ		
	1	Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда	180
	2	Ознакомление с кабельными цехами и участками	
	3	Работа с технической документацией	
	4	Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий	
	5	Ознакомление с оборудованием ИТКС	
	6	Изучение и работа с контрольно-измерительным оборудованием	
	7	Самостоятельная работа на закрепленном рабочем месте	
	8	Выполнение индивидуального задания по практике	
	9	Участите в аварийных и профилактических работах, проводимых на кабельном участке	
	10	Обобщение материала, оформление отчета, сдача зачета	
Всего по ПМ			514

3.2.2. Содержание практической подготовки по **ПМ.02.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе, криптографических средств защиты**

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			
МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			
Тема 1.1. Обеспечение безопасности операционных систем	Содержание учебного материала		
	Лабораторные работы		
	1	Занятие 16. Средства идентификации аутентификации операционных систем	8
	2	Занятие 17. Настройка локальной политики безопасности операционной системы. Политика паролей. Политики учетных записей.	
	3	Занятие 18. Назначение прав пользователя.	
	4	Занятие 19. Настройка изолированной среды	
	Практические занятия		
	1	Занятие 20. Параметры безопасности. Политика аудита	10
	2	Занятие 21. АПМДЗ Криптон: инициализация системного администратора, инициализация пользователя, проверка целостности среды	
	3	Занятие 22. Аппаратные средства шифрования Криптон: настройка, эксплуатация	
	4	Занятие 23. Программные средства шифрования. Защищенные контейнеры.	
	5	Занятие 24. Восстановление информации типовыми средствами	
Тема 1.2. Технологии разграничения доступа	Содержание учебного материала		
	Практические занятия		
	6	Занятие 43. Программы надежного удаления информации	10
	7	Занятие 44. Архивирование информации	
	8	Занятие 45. Программные средства резервного копирования. Настройка RAID-массивов	
	9	Занятие 46. Инсайдерская информация. Программы сбора информации о ПК	
	10	Занятие 47. Настройка межсетевого экрана	
	Содержание учебного материала		26

Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Лабораторные работы		
	5	Занятие 61. Примеры политик безопасности VPN	26
	6	Занятие 62. Протоколы защиты данных канального уровня (PPTP, L2F и L2TP). Сравнительный анализ протоколов защиты на канальном уровне.	
	7	Занятие 63. Защита данных на сетевом уровне (Протокол IPSec). Протоколы туннельного и транспортного режимов.	
	8	Занятие 64. Защита на сеансовом уровне (Протоколы SSL, TLS, SOCKS)	
	9	Занятие 65. Инфраструктура открытых ключей (ИОК). Модели APKI и PKIX	
	10	Занятие 66. Сертификат открытого ключа. Формат сертификации открытого ключа. Аннулирование сертификатов	
	11	Занятие 67. Реализация алгоритмов скоростной криптозащиты	
	12	Занятие 68. VPN на базе сетевых операционных систем	
	13	Занятие 69. VPN на базе специализированного программного обеспечения	
	14	Занятие 70. VPN на базе аппаратных средств.	
	15	Занятие 71. Использование токена на рабочем месте администратора	
	16	Занятие 72. Установка и настройка СКЗИ «КриптоПро CSP»	
	17	Занятие 73. Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	
Тема 1.4. Технологии обнаружения вторжений	Содержание учебного материала		
	Лабораторные работы		2
	18	Занятие 89. Проектирование стенда для реализации IDS	
	Практические занятия		10
	11	Занятие 90. Настройка интерфейсов виртуальных машин	
	12	Занятие 91. Конфигурация правила для СОВ	
	13	Занятие 92. Развертывание открытых списков правил	
	14	Занятие 93. Подключение средства мониторинга	
	15	Занятие 94. Включение режима блокировки	
Курсовой проект	Обязательные аудиторные учебные занятия по курсовому проекту		30
	1	Введение. Выдача заданий	
	2	Анализ поставленной задачи	
	3	Определение защищаемых информационных активов. Категорирование информации	
	4	Определение уязвимостей и угроз	

	5	Анализ и выбор возможных решений по защите	
	6	Анализ механизмов защиты	
	7	Анализ требуемых компонентов	
	8	Проектирование модели угроз	
	9	Настройка компонентов защиты	
	10	Конфигурирование пользовательских задач	
	11	Проектирование эксперимента по внедрению системы защиты	
	12	Нормативно-правовое обеспечение проекта	
	13	Расчет индекса ROSI	
	14	Подготовка пояснительной записки к курсовому проекту	
	15	Защита курсового проекта	
УП.02.Учебная практика МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	Виды работ:		
	1	Работа с учетными записями пользователей	72
	2	Настройка параметров безопасности ОС	
	3	Управление хранением данных.	
	4	Архивация данных	
	5	Восстановление данных	
	6	Аудит ресурсов ОС	
	7	Аудит событий ОС	
	8	Управление доступом в Linux	
	9	Управление доступом в Windows	
	10	Средства аутентификации операционных систем	
	11	Управление средствами аутентификации в Linux	
	12	Управление средствами аутентификации в Windows	
	13	Документирование политики безопасности	
	14	Выбор, подключение, настройка межсетевого экрана	
	15	Выбор, подключение, настройка межсетевого экрана	
	16	Администрирование межсетевого экрана	
	17	Ознакомление, подключение, настройка системы резервного копирования	
	18	Ознакомление, подключение, настройка системы резервного копирования	
	19	Администрирование системы резервного копирования	
	20	Администрирование системы резервного копирования	

	21	Ознакомление, подключение, настройка системы антивирусной защиты	
	22	Администрирование системы антивирусной защиты.	
	23	Изучение методов комплексного исследования объекта информатизации	
	24	Изучение информации циркулирующей в корпоративной информационной системе	
	25	Изучение построения системы защиты информации на основе нормативных актов и методических указаний	
	26	Изучение построения системы защиты информации на основе нормативных актов и методических указаний	
	27	Построение модели угроз ИСПДн	
	28	Определение вероятности реализации угроз безопасности в информационной системе персональных данных	
	29	Изучение действующей нормативной документации объекта информатизации	
	30	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	31	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	32	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	33	Разработка КСЗИ информационной системы: сбор данных	
	34	Разработка КСЗИ информационной системы: выбор технологий	
	35	Разработка КСЗИ информационной системы: разработка модели	
	36	Разработка КСЗИ информационной системы: оформление решения	
Раздел 2.Криптографическая защита информации			
МДК 02.02.Криптографическая защита информации			
Тема 2.1. Основы криптографических методов защиты информации	Содержание учебного материала		
	Практические занятия		14
	1	Занятие 16. Стеганографические методы скрытия информации	
	2	Занятие 17. Применение методов шифрования перестановкой	
	3	Занятие 18. Применение методов шифрования заменой	
	4	Занятие 19. Применение методов шифрования многоалфавитной замены	
	5	Занятие 20. Криптоанализ методов перестановки	
	6	Занятие 21. Криптоанализ методов замены	
	7	Занятие 22. Компьютерное шифрование	
Тема 2.2. Современные стандарты шифрования	Содержание учебного материала		18
	Практические занятия		10

	6	Занятие 32. Алгоритм Диффи-Хелмана	
	7	Занятие 33. Стандарт симметричного шифрования AES RIJNDAEL	
	8	Занятие 34. Генерация простых чисел, используемых в асимметричных системах шифрования	
	9	Занятие 35. Криптографические хэш-функции. Аутентификация.	
	10	Занятие 36. Шифрование методом скользящей перестановки	
	Лабораторные работы		
	1	Занятие 37. Изучение программных продуктов защиты информации. Программа PGP (Pretty Good Privacy)	10
	2	Занятие 38. Шифр Плейфера.	
	3	Занятие 39. Российский стандарт хэш-функции ГОСТ Р 34.11-94	
	4	Занятие 40. Криптосистема RSA	
	5	Занятие 41. Электронная цифровая подпись	
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	Содержание учебного материала		28
	Лабораторные работы		
	6	Занятие 74. Разработка схемы простого пароля	
	7	Занятие 75. Разработка схемы динамического пароля	10
	8	Занятие 76. Сертификаты открытого ключа	
	9	Занятие 77. Настройка и администрирование токена	
	10	Занятие 78. Настройка сервисов Рутокен	
УП.02.Учебная практика МДК.02.02. Криптографическая защита информации	Виды работ		
	1	Настройка и администрирование токена	
	2	Настройка сервисов Рутокен-PinPad	
	3	Настройка сервисов Рутокен-ЭЦП	
	4	Настройка сервисов Рутокен–Bluetooth	
	5	Настройка сервисов Рутокен–S	
	6	Разработка алгоритма PGP	36
	7	Изучение протоколов SSL, TLS, IPSec	
	8	Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	
	9	Составление алгоритма хеш-функции	
	10	Составление алгоритма шифра	
	11	Подключение, установка драйверов, настройка программных средств шифрования Криптон.	

	12	Администрирование программных средств шифрования Криптон	
	13	Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон.	
	14	Администрирование аппаратных средств шифрования Криптон.	
	15	Инфраструктуры открытых ключей и стандарт X.509	
	16	Защита электронного документооборота с использованием электронной цифровой подписи	
	17	Программная реализация ГОСТ Р 34.12- 2015	
	18	Стандарты информационной безопасности в Интернете (IETF, RFC).	
ПП.02.Производственная практика (по профилю специальности)	Виды работ		180
	1	Инструктаж по технике безопасности	
	2	Ознакомление с рабочим местом	
	3	Ознакомление с организационной структурой предприятия	
	4	Резервное копирование информации	
	5	Восстановление данных	
	6	Проверка копий на предприятии, изучение технологии резервного копирования	
	7	Защита информации от несанкционированного доступа	
	8	Регистрация и учёт входа/выхода субъектов системы в/из системы (узла сети)	
	9	Учёт носителей информации	
	10	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	
	11	Работа с антивирусами	
	12	Обновление антивирусных программ	
	13	Защита почтовых ящиков	
	14	Шифрование конфиденциальной информаци	
	16	Работа в программе cryptoapi	
	17	Работа в программе Windows Defender	
	18	Изучение дискреционного принципа контроля доступа к информации	
	19	Создание системы защиты персональных данных	
	20	Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ	
	21	Участие в организации работ по защите персональных компьютеров на предприятии	
	22	Участие в организации работ по защите локальных сетей на предприятии	
	23	Участие в организации работ по защите работ в глобальной сети интернет на предприятии	

	24	Работа с криптографическими средствами защиты информации	
	25	Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети.	
	26	Администрирование систем безопасности беспроводной защищенной локальной сети.	
	27	Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей.	
	28	Выбор программных средств шифрования в соответствии с решаемой задачей	
	29	Подключение, установка драйверов, настройка программных средств абонентского шифрования	
	30	Администрирование внедренных средств	
	31	Настройка средств электронной подписи	
	32	Администрирование средств электронной подписи	
	33	Администрирование средств PKI	
	34	Сдача рабочего места	
	35	Подготовка дневника и аттестационного листа по практике	
	36	Подготовка и сдача отчета по практике	
Всего по ПМ			428

3.2.3. Содержание практической подготовки по **ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты**

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект)		Объем часов
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты			
МДК.03.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты			
Тема 1.2. Общие положения защиты информации техническими средствами	Содержание учебного материала		
	Практические занятия		4
	1	Занятие 8. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	
	2	Занятие 9. Обоснование необходимости создания подсистемы технической защиты инфокоммуникационной системы на основе нормативных и методических документов.	
Тема 1.3. Технические каналы утечки информации	Содержание учебного материала		
	Практические занятия		16
	3	Занятие 16. Особенности утечки информации в проводных линиях связи.	
	4	Занятие 17. Особенности утечки информации в беспроводных линиях связи.	
	5	Занятие 18. Исследование уязвимостей и построение модели угроз объекта защиты	
	6	Занятие 19. Исследование возможностей системы оценки защищенности оптических линий связи	
	7	Занятие 20. Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН	
	8	Занятие 21. Исследование возможностей системы оценки защищенности выделенных помещений	
	9	Занятие 22. Оценка защищенности информации по акустическому каналу.	
	10	Занятие 23. Оценка защищенности информации по электромагнитному каналу.	
	Содержание учебного материала		

Тема 1.6. Системы защиты от утечки информации	Практические занятия		18
	11	Занятие 55. Определение каналов утечки ПЭМИН	
	12	Занятие 56. Работа с оборудованием по защите от утечки по ПЭМИН	
	13	Занятие 57. Работа с оборудованием по защите от утечки по ПЭМИН	
	14	Занятие 58. Определение утечки по цепям электропитания и заземления	
	15	Занятие 59. Защита от утечки по цепям электропитания и заземления	
	16	Занятие 60. Определение утечки информации по акустическому каналу	
	17	Занятие 61. Работа с оборудованием по защите от утечки по акустическому каналу	
	18	Занятие 62. Определение утечки информации по виброакустическому каналу	
	19	Занятие 63. Работа с оборудованием по защите от утечки по виброакустическому каналу	
	Лабораторные работы		32
	1	Занятие 64. Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.	
	2	Занятие 65. Поиск и локализация скрытых видеокамер	
	3	Занятие 66. Исследование методов защиты сотовых телефонов от несанкционированного прослушивания	
	4	Занятие 67. Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов	
	5	Занятие 68. Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора	
	6	Занятие 69. Инженерно-техническая защита информации.	
	7	Занятие 70. Выявление и фиксация следов противоправной деятельности, связанной с использованием компьютерной деятельности	
	8	Занятие 71. Исследование уровня побочного электромагнитного излучения ПК	
	9	Занятие 72. Снятие диаграммы направленного микрофона	
	10	Занятие 73. Исследование спектра речевого сигнала	
	11	Занятие 74. Определение уровня побочного излучения в канале электросвязи	
	12	Занятие 75.Определение уровня побочного излучения в канале виброакустики	
	13	Занятие 76. Измерение уровня маскирующего виброакустического шума	
	14	Занятие 77. Измерение уровня маскирующего цифрового шума	
	15	Занятие 78. Испытание учебной аудитории на утечку информации по каналу ПЭМИН	

	16	Занятие 79.Испытание учебной аудитории на утечку информации по виброакустическому каналу	
Курсовое проектирование	Обязательные аудиторные учебные занятия по курсовому проекту		30
	1	Занятие 80. Введение. Выдача заданий	
	2	Занятие 81. Анализ поставленной задачи	
	3	Занятие 82. Определение защищаемых информационных активов. Категорирование информации	
	4	Занятие 83. Определение уязвимостей и угроз	
	5	Занятие 84. Анализ и выбор возможных решений по защите	
	6	Занятие 85. Анализ механизмов защиты	
	7	Занятие 86. Анализ требуемых компонентов	
	8	Занятие 87. Проектирование модели угроз	
	9	Занятие 88. Настройка компонентов защиты	
	10	Занятие 89. Конфигурирование пользовательских задач	
	11	Занятие 90. Проектирование эксперимента по внедрению системы защиты	
	12	Занятие 91. Нормативно-правовое обеспечение проекта	
	13	Занятие 92. Расчет индекса ROSI	
	14	Занятие 93. Подготовка пояснительной записки к курсовому проекту	
	15	Занятие 94. Защита курсового проекта	
Раздел 2. Физическая защита линий связи ИТКС			
МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей			
Тема 2.1. Цели и задачи физической защиты объектов информатизации	Содержание учебного материала		
	Практические занятия		4
	1	Занятие 3. Исследование возможностей СЗИ «Страж NT»	
	2	Занятие 4. Исследование программной среды «Страж NT»	
Тема 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание учебного материала		
	Практические занятия		10
	3	Занятие 7. Управление пользователями «Страж NT», учет пользователей «Страж NT»	
	4	Занятие 8. Избирательное управление «Страж NT»	
	5	Занятие 9. Сортировка и поиск с «Страж NT»	
	6	Занятие 10. Редактирование пользователей «Страж NT»	
	7	Занятие 11. Изменение настроек «Страж NT»	
	Содержание учебного материала		

Тема 2.3. Система обнаружения комплекса инженерно-технических средств физической защиты	Практические занятия		8
	8	Занятие 14. Исследование возможностей «Сигурд М19»	
	9	Занятие 15. Подготовка к работе «Сигурд М19»	
	10	Занятие 16. Поиск сигналов ПЭМИН «Сигурд М19»	
	11	Занятие 17. Анализ сигналов «Сигурд М19»	
Тема 2.4. Система контроля и управления доступом	Содержание учебного материала		
	Практические занятия		12
	12	Занятие 25. Обоснование необходимости создания СКУД объекта информатизации на основе нормативных и методических документов.	
	13	Занятие 26. Модели нарушителей физической безопасности объекта информатизации.	
	14	Занятие 27. Разработка топологии многозональной и многорубежной системы физической защиты объекта	
	15	Занятие 28. Разработка структурной и функциональной схем СКУД.	
	16	Занятие 29. Разработка основных организационных документов службы режима предприятия.	
	17	Занятие 30. Разработка методик контроля эффективности СКУД.	
Тема 2.5. Система телевизионного наблюдения	Содержание учебного материала		
	Практические занятия		4
	18	Занятие 33. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
	19	Занятие 34. Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.6. Система сбора, обработки, отображения и документирования информации	Содержание учебного материала		
	Практические занятия		4
	20	Занятие 37. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации	
	21	Занятие 38. Сравнение отечественных ССОИ	
Тема 2.7. Система воздействия	Содержание учебного материала		
	Практические занятия		6
	22	Занятие 40. Исследование возможностей радиолокатора NR-900EMS	
	23	Занятие 41. Исследование возможностей прибора ST 033P Пиранья	
	24	Занятие 42. Исследование возможностей анализатора спектра OSCOR Green	
	Содержание учебного материала		

Тема 2.8. Применение инженерно-технических средств физической защиты	Практические занятия		6
	25	Занятие 51. Проведение анализа защищаемой в кабинете руководителя информации	
	26	Занятие 52. Моделирование угроз воздействия на источники информации	
	27	Занятие 53. Разработка и осуществление мер по предотвращению проникновения злоумышленника к источникам информации	
Тема 2.9. Эксплуатация инженерно-технических средств физической защиты	Содержание учебного материала		
	Лабораторные работы		16
	1	Занятие 64. Исследование возможностей имитатора АВРОРА-3	
	2	Занятие 65. Исследование возможностей комплекса КРОНА-ПРО	
	3	Занятие 66. Исследование возможностей приемника СКОРПИОН-XL	
	4	Занятие 67. Исследование принципов работы индикатора поля РИЧ-8	
	5	Занятие 68. Исследование принципов работы индикатора поля MFP-8000	
	6	Занятие 69. Исследование принципов работы индикатора поля ST-107	
	7	Занятие 70. Исследование принципов работы индикатора поля PST-165	
	8	Занятие 71. Исследование возможностей системы ШЕПОТ	
УП.03.Учебная практика	Виды работ		
	1	Занятие 1. Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике.	108
	2	Занятие 2. Монтаж различных типов датчиков.	
	3	Занятие 3. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	
	4	Занятие 4. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации	
	5	Занятие 5. Рассмотрение системы контроля и управления доступом	
	6	Занятие 6. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование	
	7	Занятие 7. Рассмотрение датчиков периметра, их принципов работы	
	8	Занятие 8. Выполнение звукоизоляции помещений системы зашумления	
	9	Занятие 9. Реализация защиты от утечки по цепям электропитания и заземления	
	10	Занятие 10. Рассмотрение принципов работы ЛВП-10 Электромагнитный вибропреобразователь к ЛГШ-404 (для окон, стен, труб)	
	11	Занятие 11. Рассмотрение многозонной системы обнаружения и блокирования мобильных средств связи для образовательных учреждений	

	12	Занятие 12. Монтаж различных типов датчиков	
	13	Занятие 13. Рассмотрение устройств обнаружения скрытых видеокамер «Алмаз»	
	14	Занятие 14. Применение промышленных осциллографов, частотомеров и генераторов акустического шума, двухканального генератора, системы постановки виброакустических помех и другого оборудования для защиты информации.	
	15	Занятие 15. Рассмотрение системы контроля и управления доступом	
	16	Занятие 16. Рассмотрение принципов работы программно-аппаратного комплекса защиты объектов информационных технологий от разведки ПЭМИ, 0,009 - 1000 МГц	
	17	Занятие 17. Рассмотрение датчиков периметра, их принципов работы	
	18	Занятие 18. Изучение средств перехвата информации	
	19	Занятие 19. Микрофоны	
	20	Занятие 20. Акустические антенны	
	21	Занятие 21. Выбор типа микрофона и места его установки	
	22	Занятие 22. Изучение устройств подавления микрофонов	
	23	Занятие 23. Изучение устройств для перехвата речевой информации в проводных каналах	
	24	Занятие 24. Изучение оптико-акустической аппаратуры перехвата речевой информации	
	25	Занятие 25. Оптико-механические приборы	
	26	Занятие 26. Приборы ночного видения	
	27	Занятие 27. Средства скрытой фотосъемки	
	28	Занятие 28. Зоны подключения в линиях связи	
	29	Занятие 29. Перехват телефонных переговоров в зонах «А», «Б», «В», «Г», «Д», «Е»	
	30	Занятие 30. Изучение перехвата сообщений в каналах сотовой связи	
	31	Занятие 31. Методы поиска закладных устройств как физических объектов и электронных средств	
	32	Занятие 32. Панорамные приемники	
	33	Занятие 33. Аппаратура контроля и защиты линии связи	
	34	Занятие 34. Средства создания акустических и электромагнитных маскирующих помех	
	35	Занятие 35. Измерение токов, напряжений и сопротивлений	
	36	Занятие 36. Исследование двухполюсников с помощью мультиметра	
	37	Занятие 37. Прямые и косвенные однократные измерения	
	38	Занятие 38. Обработка и представление однократных измерений при наличии систематической погрешности	

	39	Занятие 39. Стандартная обработка результатов прямых измерений с многократным наблюдением	
	40	Занятие 40. Обработка результатов прямых измерений с многократным наблюдением при наличии грубых погрешностей	
	41	Занятие 41. Определение погрешности цифрового вольтметра сличения и прямых измерений	
	42	Занятие 42. Измерение мощности и силы постоянного электромагнитного тока	
	43	Занятие 43. Измерение постоянного напряжения методом компенсации	
	44	Занятие 44. Измерение переменного электрического напряжения	
	45	Занятие 45. Измерение частоты и периода электрических сигналов	
	46	Занятие 46. Терморезисторные измерительные преобразователи. Измерители температуры	
	47	Занятие 47. Емкостные измерительные преобразователи. Измерение размера	
	48	Занятие 48. Индуктивные измерительные преобразователи. Измерение перемещения	
	49	Занятие 49. Термоэлектрические измерительные преобразователи. Измерение температуры	
	50	Занятие 50. Пьезоэлектрические измерительные преобразователи. Измерение переменных ускорений	
	51	Занятие 51. Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами	
	52	Занятие 52. Применение существующих способов выявления опасности целостности информации	
	53	Занятие 53. Выявление технических каналов утечки информации	
	54	Занятие 54. Оформление отчета по учебной практике	
ПП.03.Производственная практика (по профилю специальности)	Виды работ		180
	1	Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике	
	2	Определение исходных данных по защищаемому объекту и плана работ по созданию системы защиты речевой информации (СЗРИ)	
	3	Выявление технических каналов утечки (ТКУ) речевой информации с использованием современных средств контроля и контрольно-измерительной аппаратуры	
	4	Подготовка предложений в проект технического задания на создание СЗРИ, в том числе специального защищенного (экранированного) помещения (СЗП)	
	5	Разработка рекомендаций по совершенствованию мер защиты речевой информации и предложения по корректировке СЗРИ и СЗП	

	6	Монтаж средств защиты информации и их настройка, инструментальная оценка эффективности защиты речевой информации и электромагнитного экранирования СЗП
	7	Опытная эксплуатация СЗРИ и СЗП в целях проверки их работоспособности
	8	Участие в монтаже средств охраны и безопасности, инженерной защиты
	9	Анализ уязвимости системы
	10	Выявление ПЭМИН в информационной системе и защита от них
	11	Восстановление информации при перехвате ПЭМИН
	12	Предотвращение утечки информации через ПЭМИН ПК
	13	Организационные мероприятия по технической защите информации от утечки по каналам ПЭМИН
	14	Организационные мероприятия по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам ПЭМИН
	15	Применение активных методов защиты информации от утечки по каналам ПЭМИН
	16	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами
	17	Оценка защищенности основных технических средств в составе автоматизированной системы от утечки информации по каналу побочных электромагнитных излучений
	18	Оценка защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от её утечки за счет наводок информативного сигнала
	19	Участие в обслуживании технических средств защиты информации
	20	Выполнение подбора, настройки и применения технических средств защиты информации
	21	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения
	22	Использование средств охраны и безопасности объекта
	23	Организация и реализация технической охраны объектов
	24	Парольная аутентификация в системах ИБ и PIN-код в СКУД
	25	Участие в организации работ по технической защите конфиденциальной информации
	26	Контроль доступа к неструктурированным данным
	27	Внутренний контроль обработки ПДн
	28	Контроль за соответствием обработки ПДн
	29	Участие в перехвате побочных электромагнитных излучений

	30	Поиск и измерение ПЭМИ монитора на ЭЛТ (монитора на ЖК) в автоматическом и режиме управляющей программы
	31	Составление протокол исследования с помощью расчетной программы
	32	Съем наводок ПЭМИ ТСОИ с соединительных линий ВТСС и посторонних проводников
	33	Защита информации в АСУ
	34	Защита информации при передаче данных
	35	Защита информации ограниченного доступа
	36	Защита информации на жестком диске
	37	Защита информации при использовании электронной почты
	38	Комплексная защита информации в корпоративных системах
	39	Защита информации в компьютерных сетях
	40	Защита информации в локальных вычислительных сетях
	41	Защита информации в VPN-сетях
	42	Защита информации от несанкционированного доступа в сетях
	43	Контроль доступа к информации
	44	Управление доступом к информации
	45	Техническая защита информации на предприятии
	46	Инженерно-техническая защита информации на предприятии
	47	Защита информации, составляющей коммерческую тайну
	48	Разработка модели КСЗИ
	49	Технологическое и организационное построение КСЗИ
	50	Кадровое обеспечение функционирования КСЗИ
	51	Участие в эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения
	52	Участие в эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам
	53	Установка и настройка средств защиты информации
	54	Участие в монтаже технических средств защиты информации
	55	Участие в монтаже средств охраны и безопасности, технической охраны объектов
	56	Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам
	57	Настройка системы защиты информации от съема и утечки по техническим каналам

	58	Выявление технических каналов
	59	Поиск ЗУ и других технических каналов
	60	Выявление путей утечки информации в ИС
	61	Оценка уязвимости системы
	62	Участие в монтаже средств охраны и безопасности и систем видеонаблюдения
	63	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам
	64	Определение требований к системе защиты информации
	65	Проектирование системы защиты информации
	66	Разработка эксплуатационной документации на систему защиты информации
	67	Установка и настройка средств защиты информации
	68	Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
	69	Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
	70	Испытания и опытная эксплуатации системы защиты информации
	71	Подтверждение соответствия системы защиты информации
	72	Выполнение мероприятий по предотвращению несанкционированного доступа к информации
	73	Оценка эффективности использованных мер и средств защиты информации
	74	Контроль эффективности защиты информации
	75	Защита информации обрабатываемой ТСПИ от утечки по техническим каналам
	76	Защита от утечки информации по телефонному каналу
	77	Защита от утечки информации по электросетевому каналу
	78	Защита от утечки информации по вибрационному каналу
	79	Защита от утечки информации по проводному каналу
	80	Формирование требований к системе защиты информации
	81	Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации
	82	Изучение порядка применения нормативных правовых актов
	83	Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами

	84	Выявление технических каналов утечки информации	
	85	Применение существующих способов выявления опасности целостности информации	
	86	Анализ объектов информатизации предприятий, учреждений, организаций	
	87	Анализ ресурсов обеспечения инженерно-технической защиты информации	
	88	Изучение основных этапов проектирования системы защиты информации техническими средствами	
	89	Проектирование рабочих проектов по системе пожарно-охранной сигнализации, видеонаблюдения, СКУД	
	90	Оформление отчета	
Всего по ПМ			458

3.2.4. Содержание практической подготовки по **ПМ.04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (Оператор электронно-вычислительных и вычислительных машин)**

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)		Объем часов
Раздел 1. Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»			
МДК 04.01 Технология выполнения работ			
Тема 1.1.Работа с устройствами компьютерной системы	Лабораторные работы		6
	1	Занятие 1. Соблюдение техники безопасности при работе на ЭВМ	
	2	Занятие 2. Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ	
	3	Занятие 3. Работа с дополнительными внешними устройствами ПК: устройство, подключение и настройка	
Тема 1.2.Работа с программным обеспечением компьютерной системы	Лабораторные работы		6
	4	Занятие 4. Подготовка внутреннего накопителя ПК к установке ПО	
	5	Занятие 5. Установка операционной среды, настройка интерфейса ОС	
	6	Занятие 6. Установка и удаление прикладного ПО. Настройка параметров совместимости	
Тема 1.3.Диагностика неисправностей системы, ведение документации	Лабораторные работы		4
	7	Занятие 7. Диагностика ПК. Базовые настройки системы ввода-вывода ПК	
	8	Занятие 8. Диагностика простейших неисправностей ПК, периферийного оборудования и компьютерной оргтехники	
Тема 2.1.Работа в текстовом процессоре	Лабораторные работы		
	9	Занятие 9. Работа в текстовом процессоре. Создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов	2
Тема 2.2.Работа в редакторе электронных таблиц	Лабораторные работы		2
	10	Занятие 10. Создание и форматирование таблицы в редакторе электронных таблиц	
Тема 2.3.Работа в программе подготовки и просмотра презентаций	Лабораторные работы		2
	11	Занятие 11. Построение презентации	

Тема 2.4.Работа в системе управления базами данных	Лабораторные работы		2
	12	Занятие 12. Создание таблиц базы данных	
Тема 2.5.Работа в графических редакторах	Лабораторные работы		2
	13	Занятие 13. Рисование объектов средствами графического редактора.	
Тема 3. Использование ресурсов технологий и сервисов Интернета			
Тема 3.1.Работа с ресурсами Интернета	Лабораторные работы		4
	14	Занятие 14. Создание и обмен письмами электронной почты	
	15	Занятие 15. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера.	
Тема 4.1. Защита информации при работе с офисными приложениями	Содержание учебного материала		
	Лабораторные работы		4
	16	Занятие 18. Установка антивирусных программ и поиск вирусов	
	17	Занятие 19. Использование Восстановления ОС	
УП.04.Учебная практика	Виды работ		72
	1	Безопасная организация рабочего места оператора ЭВМ.	
	2	Выполнение разборки системного блока и ТО компонентов.	
	3	Изучение компонентов ПК и сборка системного блока.	
	4	Подключение и запуск ПК. Первичные настройки ПК	
	5	Изучение аппаратных характеристик ПК и характеристик ОС ПК.	
	6	Установка и замена расходных материалов для оргтехники.	
	7	Управление файлами данных ПК	
	8	Создание виртуального жесткого диска	
	9	Обслуживание жестких дисков в ОС	
	10	Создание комплексных документов в текстовом процессоре	
	11	Создание формул и уравнений в документах в текстовом процессоре.	
	12	Создание диаграмм в документах в текстовом процессоре.	
	13	Организация расчетов в редакторе электронных таблиц	
	14	Создание электронной книги. Относительная и абсолютная адресации в редакторе электронных таблиц.	
	15	Связанные таблицы. Расчет промежуточных итогов в редакторе электронных таблиц	
	16	Подбор параметра. Организация обратного расчета в редакторе электронных таблиц	
	17	Задачи оптимизации (поиск решения) в редакторе электронных таблиц	

	18	Связи между файлами и консолидация данных в редакторе электронных таблиц	
	19	Экономические расчеты в редакторе электронных таблиц	
	20	Обработка объектов слайдов презентации	
	21	Настройка анимации объектов в программе подготовки и просмотра презентаций	
	22	Редактирование и модификация таблиц базы данных в СУБД.	
	23	Создание пользовательских форм для ввода данных в СУБД.	
	24	Работа с данными с использованием запросов в СУБД.	
	25	Создание отчетов в СУБД.	
	26	Работа с эффектами в графическом редакторе	
	27	Вставка и редактирование готового изображения в графическом редакторе.	
	28	Настройка пользователей и групп в ОС	
	29	Настройка Резервного копирования ОС	
	30	Автоматизация процесса управления и обслуживания ОС	
	31	Безопасный режим ОС	
	32	Создание архивов из имеющихся файлов.	
	33	Локальные политики безопасности	
	34	Выполнение схемы классификации компьютерных сетей с использованием прикладных ПС	
	35	Настройка показа и демонстрация результатов работы средствами мультимедиа	
	36	Оформление отчетной документации в соответствии с перечнем работ	
ПП.04.Производственная практика (по профилю специальности)	Виды работ		
	1	Ознакомление со структурой предприятия	72
	2	Прохождение инструктажа по технике безопасности охране труда	
	3	Приемка рабочего места	
	4	Подготовка рабочего места	
	5	Инсталляция системного программного обеспечения	
	6	Инсталляция и настройка прикладного программного обеспечения	
	7	Обслуживание прикладного программного обеспечения отраслевой направленности	
	8	Применение офисного программного обеспечения в соответствии с прикладной задачей	
	9	Работа с программным обеспечением и ресурсами ЛВС	
	10	Применение программно-аппаратных комплексов для защиты информационных активов от несанкционированного доступа	
	11	Сдача рабочего места	

	12	Оформление документации по практике	
Всего по ПМ			178

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ

4.1.Требования к минимальному материально-техническому обеспечению

Лаборатория «Защиты информации от утечки по техническим каналам». Лаборатория оснащена средствами защиты информации от утечки по акустическому (виброакустическому) каналу; средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок;

шумогенераторы;
комплексный поисковый прибор;
прожигатели телефонных линий;
устройство обнаружения скрытых видеокамер;
виброакустические генераторы;
подавители диктофонов;
подавители устройств сотовой связи;
устройство защиты аналоговых сигналов;
устройство защиты цифровых сигналов;

стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения, охранно-пожарной сигнализации и охраны объек-тов;

комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

4.2.Информационное обеспечение реализации программы

Нормативные документы:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя

Гостехкомиссии России от 27 октября 1995 г. № 199.
11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
13. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
от 30 августа 2002 г. № 282.
17. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
18. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
19. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
20. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
21. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
42. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
46. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
47. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

4.2.1. Электронные издания:

1. Баранова, Е.К. Основы информационной безопасности: учебник для студ. учрежд. СПО / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019.
2. Берлин, А. Н. Высокоскоростные сети связи: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
3. Берлин, А. Н. Оконечные устройства и линии абонентского участка информационной сети: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
4. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. - Москва: Горячая линия-Телеком, 2018.
5. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов. – 7-е изд., испр. – Москва: Горячая Линия–Телеком, 2018.
6. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.
7. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - Москва: Форум: ИНФРА-М, 2018.
8. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020.
9. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — Москва: РИОР: ИНФРА-М, 2020.
10. Портнов, Э. Л. Оптические кабели связи, их монтаж и измерение: учебное пособие для вузов / Э.Л. Портнов. - Москва: Горячая линия-Телеком, 2012.
11. Программно-аппаратные средства обеспечения информационной безопасности / А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. – Москва: Горячая Линия–Телеком, 2016.
12. Родина, О.В. Волоконно-оптические линии связи: практическое руководство/О.В.Родина. - Москва: Горячая линия-Телеком, 2016.
13. Смычек, М.А. Технологические сети и системы связи: учебное пособие / М.А. Смычек. - 2-е изд. - Москва; Вологда: Инфра-Инженерия, 2019.
14. Соколов, С.А. Волоконно-оптические линии связи и их защита от внешних влияний: учебное пособие / С.А. Соколов. – М.: Инфра-Инженерия, 2019.
15. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/П.Б.Хорев. - 2-е изд., испр. и доп. - Москва: Форум: ИНФРА-М, 2020.
16. Цуканов, В.Н. Волоконно-оптическая техника: практическое руководство/ В.Н. Цуканов, М.Я. Яковлев. – Москва: Инфра-Инженерия, 2019.
17. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2020.

4.2.2. Электронные ресурсы:

1. RusCable.Ru. Энергетика. Электротехника. Связь: отраслевое электронное СМИ. – URL: http://www.ruscable.ru/.
2. Волхонский, В.В. Устройства охранной сигнализации/В.В.Волхонский; НИУ ИТМО. – Текст: электронный. - Санкт-Петербург: Университет ИТМО, 2015. – URL: https://books.ifmo.ru/book/1633/ustroystva_ohrannoy_signalizacii.htm
3. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. - Екатеринбург: Изд-во Урал. ун-та, 2019. – URL:

http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
4. Каторин, Ю.Ф. Защита информации техническими средствами: учебное пособие / Ю.Ф.Каторин, Разумовский А.В., Спивак А.И. под редакцией Ю.Ф. Каторина. – С.-Петербург: НИУ ИТМО, 2012. – URL: https://books.ifmo.ru/file/pdf/975.pdf
5. Марусина, М.Я. Метрологическое обеспечение средств измерений: учебное пособие М.Я.Марусина, В.Л.Ткалич, Р.Я.Лабковская.. – СПб: Университет ИТМО, 2019. – URL: https://books.ifmo.ru/file/pdf/2422.pdf
6. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Часть 1: Методическая разработка /А.П.Пленкин, Ю.В. Зачиняев. –URL: http://open-edu.rsu.ru/files/Методичка%20№4.pdf
7. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Оптическое волокно. Часть 2: Методическая разработка/А.П.Пленкин. - Таганрог, 2016. – URL: http://open-edu.rsu.ru/files/Методичка%20№5.pdf
8. Руководство по применению адресно-аналоговых систем пожарной сигнализации/ С.М. Щипицын, А. Н. Членов, И. В. Павлов, А. Е. Атаманов. –Москва: Систем Сенсор Фаир Детекторс, 2012// СИГМА: группа компаний: официальный сайт. – URL: http://www.sigma-is.ru/files/education/Rukovodstvo_AASPS_2012.pdf.
9. Рыжова, В.А. Проектирование и исследование комплексных систем безопасности/В.А.Рыжова; НИУ ИТМО. –С.-Петербург: НИУ ИТМО, 2013. – URL: https://books.ifmo.ru/file/pdf/1018.pdf
10. Теория информационной безопасности и методология защиты информации /Ю.А.Гатчин, В.В.Сухостат, А.С.Куракин, Ю.В.Донецкая. –2-е изд., испр. и доп. – С.-Петербург: Университет ИТМО, 2018. – URL: https://books.ifmo.ru/file/pdf/2372.pdf
11. Техническая эксплуатация линейных сооружений: учебное пособие/ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»; колледж связи. – Самара, 2017. – URL: http://ks.psuti.ru/downloads/students/distance_learning/3МТС-74,75/МДК.В.01.05%20Техническая%20эксплуатация%20линейных%20сооружений/МДК.01.05%20Учебное%20пособие.pdf
12. Энциклопедия инструментов: иллюстрированный справочник по инструментам и приборам. – URL: http://www.tools.ru/tools.htm.

4. 2.3. Дополнительные источники:

1. Андреев, В.А. Направляющие системы электросвязи: учебник для вузов. В 2 т. Т.1. Теория передачи и влияния/ В.А.Андреев, Э.Л.Портнов, Л.Н.Кочановский. - Москва: Горячая линия-Телеком, 2011.
2. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. - Москва: Юрайт, 2020.
3. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013.
4. Берлин, А. Н. Абонентские сети доступа и технологии высокоскоростных сетей: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
5. Берлин, А. Н. Телекоммуникационные сети и устройства: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
6. Ворона, В. А. Инженерно-техническая и пожарная защита объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая Линия–Телеком, 2012.
7. Ворона, В.А. Системы контроля и управления доступом/В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2013.

8. Ворона, В.А. Технические системы охранной и пожарной сигнализации /В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2012.
9. Ворона, В.А. Технические средства наблюдения в охране объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая линия-Телеком, 2011.
10. Голиков, А.М. Тестирование и диагностика в инфокоммуникационных системах и сетях [Электронный ресурс]: учебное пособие / А.М. Голиков. – М.: ТУСУР, 2016.
11. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2019.
12. Груба, И.И. Системы охранной сигнализации. Технические средства обнаружения: справочное пособие / И.И.Груба. - М.: СОЛОН-Пресс, 2013.
13. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие / А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2017.
14. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.
15. Направляющие системы электросвязи. В 2-х т. Т. 2. Проектирование, строительство и техническая эксплуатация: учебник для ВУЗов/В.А.Андреев, А.В.Бурдин, Л.Н.Кочановскии и др.; под ред. В.А.Андреева. - М.: Горячая линия-Телеком, 2010.
16. Пескин, А.Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации / А.Е. Пескин. - Москва: Горячая линия-Телеком, 2013.
17. Портнов, Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи: учебное пособие для вузов / Э.Л.Портнов. - Москва: Горячая линия-Телеком, 2013.
18. Портнов, Э.Л. Электрические кабели связи и их монтаж: учебное пособие/Э.Л.Портнов, А.Л.Зубилевич. - 2-е изд. - Москва: Горячая линия-Телеком, 2010.
19. Программно-аппаратные средства обеспечения информационной безопасности / А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. – Москва: Горячая Линия–Телеком, 2016.
20. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей: учебное пособие для вузов/Е.Б.Алексеев, В.Н.Гордиенко, В.В.Крухмалев и др.; под ред. В.Н.Гордиенко, М.С.Тверецкого. - Москва: Горячая линия-Телеком, 2017.
21. **Рябко, Б. Я.** Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. – М.: Горячая линия–Телеком, 2017.
22. Скрипник, Д.А. Общие вопросы технической защиты информации/ Д.А.Скрипник. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
23. Субботин, Е. А. Методы и средства измерения параметров оптических телекоммуникационных систем: Учебное пособие для вузов / Е.А. Субботин. - Москва: Горячая линия-Телеком, 2013.
24. Техническая диагностика современных цифровых сетей связи. Основные принципы и технические средства измерений параметров передачи для сетей PDH, SDH, IP, Ethernet и ATM/И.И. Власов, Э.В.Новиков, М.М.Птичников, Д.В.Сладких; под ред. М.М.Птичникова. - М.: Горячая линия-Телеком, 2017.
25. Чернышев, Е.И. Линейные сооружения связи: учебное пособие для студ. учрежд. СПО/Е.И.Чернышев. - Волгоград: Ин-Фолио, 2010.

Периодические издания:

1. Защита информации Inside.
2. Information Security/Информационная безопасность.
3. Электросвязь.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРАКТИЧЕСКОЙ ПОДГОТОВКИ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей	- производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; - проверять функционирование, производить регулировку и контроль основных параметров источников питания ИТКС; - измерять основные показатели и характеристики при выполнении работ по настройке, проверке функционирования и конфигурирования ИТКС;	Экспертное наблюдение
ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования ИТКС	- осуществлять техническую эксплуатацию линей- ных сооружений связи; - проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; - измерять основные параметры и характеристики при выполнении работ по диагностике технического состояния, поиска неисправностей и ремонте оборудования ИТКС;	Экспертное наблюдение
ПК 1.3. Проводить техническое обслуживание оборудования ИТКС	- осуществлять техническую эксплуатацию линей- ных сооружений ИТКС; - измерять основные параметры и характеристики при выполнении технического обслуживания оборудования ИТКС; - производить контроль и регулировку основных параметров источников питания оборудования ИТКС;	Экспертное наблюдение
ПК 1.4. Осуществлять контроль функционирования ИТКС	- проводить мониторинг и контроль функционирования оборудования ИТКС; - измерять основные параметры и характеристики оборудования ИТКС; - вести эксплуатационно-техническую документацию на оборудование ИТКС;	Экспертное наблюдение
ПК 2.1. Осуществлять установку (монтаж),	- выявлять и оценивать угрозы безопасности информации в ИТКС;	Экспертное наблюдение

настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС	- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	
ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС и их диагностику, обнаружение отказов, формировать предложения по их устранению	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-	Экспертное наблюдение

систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей	аппаратных (в том числе криптографических) средств защиты информации;	
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в ИТКС	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к	- требования техники безопасности при работе с вычислительной техникой;	Экспертное наблюдение

работе, производить инсталляцию, настройку и обслуживание программного обеспечения	- основные принципы устройства и работы компьютерных систем и периферийных устройств; - выполнять требования техники безопасности при работе с вычислительной техникой;	Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.
ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	- производить подключение блоков персонального компьютера и периферийных устройств; - производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; - диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; - выполнение требований техники безопасности при работе с вычислительной техникой; организация рабочего места оператора электронно-вычислительных и вычислительных машин - подготовка оборудования компьютерной системы к работе; - инсталляция, настройка и обслуживание программного обеспечения компьютерной системы; - управление файлами.	Экспертное наблюдение Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.
ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	- назначение и функции офисных приложений; создавать и управлять содержимым документов с помощью текстовых процессоров; - создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; - создавать и управлять содержимым презентаций с помощью редакторов презентаций; - использовать мультимедиа проектор для демонстрации презентаций; вводить, редактировать и удалять записи в базе данных; - эффективно пользоваться запросами базы данных; - создавать и редактировать графические объекты с помощью программ для обработки растровой и	Экспертное наблюдение Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.

	векторной графики; производить сканирование документов и их распознавание; - производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода; - применение офисного программного обеспечения в соответствии с прикладной задачей; - управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; - осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; - осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; - создавать и обмениваться письмами электронной почты; - использование ресурсов локальной вычислительной сети; - использование ресурсов, технологий и сервисов Интернет, основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы;	
ПК 4.4. Обеспечивать применение средств защиты информации в компьютерной системе	- осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; - осуществлять резервное копирование и восстановление данных; - выполнять архивирование информации;	Экспертное наблюдение Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение
ОК 02. Использовать современные средства	- использование различных источников, включая электронные	Экспертное наблюдение

поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение