Смоленский колледж телекоммуникаций (филиал)
Федерального государственного бюджетного образовательного
учреждения высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

УТВЕРЖДАЮ
Зам. директора по учебной работе
СКТ(ф)СПбГУТ
_____ И.А. Овчинникова
«14» 05 2025 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СМОЛЕНСК
Сертификат: 00F35A15D2181C25968B35D1B1F78BE7DA
Владелец: Овчинникова Ирина Александровна
Действителен: с 09.04.2026 до 03.07.2027

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ УП.03

в составе

ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

среднего профессионального образования

для специальности
11.02.15 Инфокоммуникационные сети и системы связи

г.Смоленск, 2025г.

РАССМОТРЕНО
на заседании методической
комиссии дисциплин
сетей связи
Председатель _____ Е.Н. Кожекина
Протокол № 11 от «14» 05 2025 г.

СОГЛАСОВАНО
Начальник отдела защиты информации
Министерства цифрового развития
Смоленской области
_____ А.Н.Калугин
«14» 05. 2025 г.

СОГЛАСОВАНО
Методист _____ О.Г. Ряска
«14» 05 2025 г

Составитель: Грубник Е.М. – преподаватель СКТ (ф) СПбГУТ.

Рабочая программа учебной практики разработана на основе ФГОС среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утвержденного приказом Министерства просвещения Российской Федерации № 675 от 05.08.2022 года (ред. от 03.07.2024).

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ В СОСТАВЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ. 03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

1.1. Область применения программы

Рабочая программа учебной практики профессионального модуля ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности по специальности 11.02.15 Инфокоммуникационные сети и системы связи в части освоения основного вида профессиональной деятельности и соответствующих профессиональных (ПК) и общих (ОК) 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
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 иностранном языках.

1.2. Цели и задачи учебной практики, требования к результатам освоения

С целью освоения указанного вида профессиональной деятельности и соответствующих профессиональных компетенций студент должен в обязательной части
иметь практический опыт
в ПО1 - анализировать сетевую инфраструктуру;
в ПО2- выявлять угрозы и уязвимости в сетевой инфраструктуре;
в ПО3 - разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;
в ПО4 - осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи;
в ПО5 - использовать специализированное программное обеспечения и оборудование для защиты инфокоммуникационных сетей и систем связи;

уметь
У 1 - классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;
У 2 - проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;
У 3 - определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;
У 4 - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
У 5 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;
У 6 - выполнять тестирование систем с целью определения уровня защищенности;
У 7 - определять оптимальные способы обеспечения информационной безопасности;
У 8 - проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;
У 9 - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;
У 10 - разрабатывать политику безопасности сетевых элементов и логических сетей;
У 11 - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
У 12 - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;
У 13 - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
У 14 - защищать базы данных при помощи специализированных программных продуктов;
У 15 - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами;
знать:
З 1 - принципы построения информационно-коммуникационных сетей;
З 2 - международные стандарты информационной безопасности для проводных и беспроводных сетей;
З 3 - нормативно - правовые и законодательные акты в области информационной безопасности;
З 4 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;
З 5 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
З 6 - способы и методы обнаружения средств съёма информации в радиоканале;
З 7 - классификацию угроз сетевой безопасности;
З 8 - характерные особенности сетевых атак;
З 9 - возможные способы несанкционированного доступа к системам связи;
З 10 - правила проведения возможных проверок согласно нормативных документов ФСТЭК;
З 11 - этапы определения конфиденциальности документов объекта защиты;
З 12 - назначение, классификацию и принципы работы специализированного оборудования;
З 13 - методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;
З 14 - методы и средства защиты информации в телекоммуникациях от вредоносных программ;
З 15 - технологии применения программных продуктов;
З 16 - возможные способы, места установки и настройки программных продуктов;
З 17 - методы и способы защиты информации, передаваемой по кабельным направляющим системам;
З 18 - конфигурации защищаемых сетей;
З 19 - алгоритмы работы тестовых программ;

З 20 - средства защиты различных операционных систем и среды передачи информации;
З 21 - способы и методы шифрования (кодирование и декодирование) информации.
В вариативной части
уметь
У 16 - проводить мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры;
У 17 - администрировать наложенные программно-аппаратных средства защиты информации от НСД;
У 18 - применять программно-аппаратные комплексы глубокого анализа трафика;
У 19 - производить выбор необходимых средств криптографической защиты информации;
У 20 - применять программные средства, реализующие основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа;
У 21 - вырабатывать рекомендации для принятия решения о модернизации системы защиты информации;
У 22 - осуществлять мероприятия по защите персональных данных;
знать
З 22 - состав работ по комплексной защите информации значимых объектов критической информационной инфраструктуры;
З 23 - концепцию инженерно-технической защиты информации;
З 24 - методы оценки угрозы инженерно-технического добывания информации;
З 25 - основные принципы организации и методы реализации технической защиты информации;
З 26 - методы аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем передачи, хранения и обработки информации;
З 27 - методы инженерного расчета размеров контролируемой зоны;
З 28 - основные требования к системам криптографической защиты;
З 29 - основные принципы организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСТЭК, ФСБ России;
З 30 - этапы проведения аудита информационной безопасности информационных систем и объектов информатизации.

1.3. Количество часов учебной практики:

Вид учебной деятельности	Объем часов
	Очная форма обучения
Максимальная учебная нагрузка (всего)	36
Обязательная аудиторная учебная нагрузка (всего)	36
Учебная практика	36
Промежуточная аттестация - 8 семестр комплексный дифференцированный зачет УП.03 и ПП.03(тестирование)	

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Результатом освоения программы учебной практики является овладение студентами основного вида деятельности - обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

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.

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 иностранном языках.

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

Код ПК	Код и наименования профессионального модуля, код и наименование МДК	Количество часов на учебную практику по ПМ и соответствующим МДК	Виды практической подготовки	Наименования тем учебной практики	Количество часов по темам
	ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи	36			
ПК 3.1 ПК 3.2 ПК 3.3	МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи	36	- реализация политик безопасности в системах и сетях на примере дискреционных и мандатных прав доступа; - проведение анализа защищенности объекта защиты информации; - проведение инструментальных проверок объекта защиты информации; - организация защиты каналов связи при подключении к защищенным ресурсам с использованием технологии ViPNet; - организация защищенного общения корпоративных пользователей (на примере ViPNet CSS Connect); - управление системой обнаружения вторжений (на примере «Континент СОВ»).	Тема 1. Реализация политик безопасности в системах и сетях на примере дискреционных и мандатных прав доступа	6
				Тема 2. Проведение анализа защищенности объекта защиты информации.	6
				Тема 3. Проведение инструментальных проверок объекта защиты информации.	6
				Тема 4. Организация защиты каналов связи при подключении к защищенным ресурсам с использованием технологии ViPNet.	6
				Тема 5. Организация защищенного общения корпоративных пользователей (на примере ViPNet CSS Connect)	6
				Тема 6. Управление системой обнаружения вторжений (на примере «Континент СОВ»)	6
	ВСЕГО часов	36			36

3.2. Содержание обучения по программе учебной практики

Код и наименование профессионального модуля, МДК и тем учебной практики	Содержание учебных занятий		Объем часов на учебную практику
ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи			36
МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи			36
- реализация политик безопасности в системах и сетях на примере дискреционных и мандатных прав доступа; - проведение анализа защищенности объекта защиты информации; - проведение инструментальных проверок объекта защиты информации; - организация защиты каналов связи при подключении к защищенным ресурсам с использованием технологии ViPNet; - организация защищенного общения корпоративных пользователей (на примере ViPNet CSS Connect); - управление системой обнаружения вторжений (на примере «Континент СОВ»)			
Тема 1. Реализация политик безопасности в системах и сетях на примере дискреционных и мандатных прав доступа	Содержание		6
	1.1.	Реализация требований РД «СВТ. Защита от НСД к информации. Показатели защищенности от несанкционированного доступа к информации» средствами операционной системы Astra Linux Special Edition.	
	1.2.	Мандатное управление доступом (передача и контроль меток конфиденциальности при передаче информации по сети), управление полномочиями (привилегиями) локальных пользователей (fly-admin-smc), управление полномочиями (привилегиями/ролями) доменных пользователей.	
	1.3.	Реализация и тестирование мандатных прав доступа и дискреционных прав доступа в Secret Net LSP.	
Тема 2. Проведение анализа защищенности объекта защиты информации.	Содержание		6
	2.1.	Комплексная проверка инфраструктуры объекта защиты информации на наличие возможных уязвимостей и поиск уязвимых мест, включая: - проверку уязвимостей локальной сети; - проверку на наличие вирусов; - анализ надежности паролей; - анализ необходимых обновлений безопасности операционных систем; - анализ настроек программного обеспечения.	
Тема 3. Проведение инструментальных проверок объекта защиты информации.	Содержание		6
	3.1.	Установка сканера безопасности ВС-6 на виртуальную машину.	
	3.2.	Управление информационными активами: сетевое сканирование хостов и сервисов, построение карт сети, назначение узлам уровня критичности, группировка по тегам, инвентаризация установленного ПО.	

Код и наименование профессионального модуля, МДК и тем учебной практики	Содержание учебных занятий		Объем часов на учебную практику
	3.3.	Выявление уязвимостей по версиям установленного ПО, использование ежедневно обновляемой базы уязвимостей, включающая данные из БДУ ФСТЭК России, NIST NVD, а также баз уязвимостей разработчиков ОС Debian, Red Hat, Arch, Ubuntu, Astra Linux и др.	
	3.4.	Подбор паролей к сетевым сервисам: использование набора встроенных словарей учетных записей и паролей, создание собственных словарей.	
	3.5	Анализ безопасности конфигурации ОС: проверка базовых настроек безопасности Linux-систем. Запуск задач по расписанию.	
Тема 4. Организация защиты каналов связи при подключении к защищенным ресурсам с использованием технологии ViPNet.	Содержание		6
	4.1.	Обеспечение защищенной работы с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей, подключающихся к сети передачи данных с помощью любых каналов связи.	
	4.2.	Настройка точечной политики информационной безопасности для конкретной ВМ или группы ВМ (блокировка всего открытого IP-трафика устройства при включенном ViPNet-соединении и управление режимом доступа приложений на устройстве в сеть ViPNet).	
	4.3	Обеспечение многоуровневой защиты устройств, использование конфигурации, блокирующей прямой доступ в Интернет для устройств, находящихся вне корпоративной сети.	
Тема 5. Организация защищенного общения корпоративных пользователей (на примере ViPNet CSS Connect)	Содержание		6
	5.1.	Установка PNet CSS Connect на мобильные устройства и ВМ персональных компьютеров.	
	5.2.	Установка серверов уведомлений и групповых чатов ViPNet CPNS и CSS ConServer (Virtual Appliance). Организация пробуждения мобильных устройств через технологию push-уведомлений и обеспечение работоспособности групповых чатов.	
	5.3.	Организация голосовых коммуникаций, отправка текстовых сообщений, в том числе с вложениями	
Тема 6. Управление системой обнаружения вторжений (на примере «Континент СОВ»)	Содержание		
	6.1.	Управление компонентами комплекса СОВ (сетевые настройки; настройка доступа; контроль узлов безопасности; учет конфигурации узлов; установка политик).	6
	6.2.	Настройка детектора компьютерных атак (в режиме Inline (интерфейсы, режим bypass, хранение трафика атаки); настройка в режиме Monitor (интерфейсы и хранение трафика атаки); создание и настройка профиля СОВ; создание и настройка правил политики СОВ; управление базой решающих правил; создание пользовательского решающего правила; управление репутационным IP-фильтром.	
	6.3.	Проведение мониторинга параметров узлов безопасности, входящих в состав комплекса «Континент СОВ».	
ВСЕГО часов:			**36**

4. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к материально-техническому обеспечению:

Обучение по программе учебной практики УП.03 осуществляется в лаборатории информационной безопасности телекоммуникационных систем.

Технические средства обучения (персональные компьютеры, оргтехника):

- автоматизированные рабочие места студентов – 10 шт. (рабочая станция с двумя мониторами Dell SE2416H 24”, клавиатурой и мышью, процессор Intel Pentium Dual Core G4620 3.7 GHz, оперативная память DDR4 16 Gb, жесткий диск 1 Tb, видеоадаптер GTX 1050 2 Gb);
- автоматизированное рабочее место преподавателя (рабочая станция с двумя мониторами Dell SE2416H 24”, клавиатурой и мышью, процессор Intel Pentium Dual Core G4620 3.7 GHz, оперативная память DDR4 16 Gb, жесткий диск 1 Tb, видеоадаптер GTX 1050 2 Gb).

Учебный сервер в колледже (аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 4 Гб; жесткий диск объемом не менее 1Тб; лицензионное или свободно распространяемое программное обеспечение).

Типовое активное оборудование: сетевые маршрутизаторы, сетевые коммутаторы, сетевые хранилища, шлюзы VPN, сетевые адаптеры и карты, сетевые контроллеры.

Специальное программное обеспечение:

1. Средства защиты от несанкционированного доступа (НСД):

- Стенд Secret Net LSP (Secret Net Studio для Linux/Secret Net LSP), разработчик ООО «Код безопасности», https://www.securitycode.ru/.
- Программный комплекс ViPNet Client 4U для защиты рабочих мест пользователей и мобильных устройств, разработчик ИнфоТеКС, https://infotecs.ru/.

2.Операционные системы:

- ВМ Astra Linux SE – разработчик ГК «Астра» (ООО «РусБИТех-Астра»), https://astralinux.ru/products.

3. Межсетевые экраны:

- Межсетевой экран ИКС (Интернет Контроль Сервер), разработчик ООО "А-Реал Консалтинг", https://xserver.a-real.ru/.
- Шлюз Безопасности Ideco UTM, разработчик ООО «Айдеко», https://ideco.ru/.
- Ideco Select, разработчик разработчик ООО «Айдеко», https://ideco.ru/.

4. Средства криптографической защиты информации (СКЗИ):

- ViPNet CryptoFile 4 (демо-версия), разработчик ИнфоТеКС, https://infotecs.ru/.
- ViPNet PKI Client (демо-версия), криптографическая защита файлов, разработчик ИнфоТеКС, https://infotecs.ru/.
- Создание и проверка ЭП: демо-версия Jinn Server 1.3.5; Jinn Client, разработчик ООО «Код безопасности», https://www.securitycode.ru/.

5. Средства доверенной загрузки:

- Высокотехнологичный программный модуль доверенной загрузки уровня UEFI BIOS ViPNet SafeBoot, разработчик ИнфоТеКС, https://infotecs.ru/.

6. Система обнаружения вторжений (IDS):

- Стенд Континент СОВ, разработчик ООО «Код безопасности», https://www.securitycode.ru/.
- Система обнаружения вторжений для рабочих станций ViPNet IDS HS, разработчик ИнфоТеКС, https://infotecs.ru/.

7.Средства защиты каналов передачи данных:

- Стенд Континент 3.М2 (АПКШ «Континент» 3.М2), разработчик ООО «Код безопасности», https://www.securitycode.ru/.
- Стенд vGate R2 (vGate), разработчик ООО «Код безопасности», https://www.securitycode.ru/.
- Демоверсия Континент-АП для Linux (версия 4.1.0.478), Континент АП/ZTN, разработчик ООО «Код безопасности», https://www.securitycode.ru/.

- Демоверсия Континент ZTN для iOS и iPadOS, разработчик ООО «Код безопасности», https://www.securitycode.ru/.

8.Средства антивирусной защиты:

- Secret Net Studio 8. Модуль: Антивирус, разработчик ООО «Код безопасности», https://www.securitycode.ru/.
- PT MultiScanner (пробная версия), разработчик компания «Позитив технолоджи», https://www.ptsecurity.com/ru-ru/.

9.Средства анализа защищенности:

- Сканер-ВС - система комплексного анализа защищенности (демо-версия), разработчик НПО «Эшелон», https://npo-echelon.ru.

10.Средства защиты мобильных устройств:

- ViPNet Mobile Client Security, разработчик ИнфоТеКС, https://infotecs.ru/.

11. Системы резервного копирования:

- Кибер Бэкап (Акронис), разработчик компания «Киберпротект», https://cyberprotect.ru/.

12.WAF средства защиты веб-приложений:

- Стенд «Континент» WAF, разработчик ООО «Код безопасности», https://www.securitycode.ru/.
- PT AF - web application firewall (WAF), разработчик компания «Позитив технолоджи», https://www.ptsecurity.com/ru-ru/

13. Защита от утечек информации (DLP):

- Staffcop Enterprise, разработчик ООО «АТОМ БЕЗОПАСНОСТЬ», https://www.staffcop.ru/enterprise/

14. Коммуникационные платформы:

- Приложение для конфиденциального общения корпоративных пользователей ViPNet CSS Connect (демо-версия), разработчик ИнфоТеКС, https://infotecs.ru/.
- Стенд Континент 3 КС (АПКШ «Континент» 3 КС), разработчик ООО «Код безопасности», https://www.securitycode.ru/.

15. Системы контроля привилегированных пользователей (PAM)

- Система контроля действий привилегированных пользователей СКДПУ НТ - комплексный продукт (демо-версия):
- СКДПУ НТ Шлюз доступа;
- СКДПУ НТ Мониторинг и аналитика;
- СКДПУ НТ Компакт;
- СКДПУ НТ Портал доступа;

Разработчик компания "АйТи БАСТИОН", https://it-bastion.com/produkt/skdpu-nt/.

16. TLS шлюзы:

- Стенд Континент TLS VPN Сервер (Континент TLS), разработчик ООО «Код безопасности», https://www.securitycode.ru/.

17. Генератор паролей:

- ViPNet Password Generator, разработчик ИнфоТеКС, https://infotecs.ru/.

4.2. Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

для преподавателей:

ОИ1. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва : Издательство Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - URL : https://urait.ru/bcode/511998.

ОИ2. Медведовский, И.Д. Практическое применение международного стандарта безопасности информационных систем ISO 17799 [Электронный ресурс] / И.Д. Медведовский. – Электрон. текст. дан. – Режим доступа: www.dsec.ru/cd-courses/iso 17799 cd.php/, свободный.

Для студентов:

ОИ1. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва : Издательство Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - URL : https://urait.ru/bcode/511998.

ОИ2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 161 с. - (Высшее образование). - ISBN 978-5-534-07248-8. - URL : https://urait.ru/bcode/512268.

ОИ3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. - 2-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 107 с. - (Высшее образование). - ISBN 978-5-534-16388-9. - URL : https://urait.ru/bcode/530927.

ОИ4. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 161 с. - (Профессиональное образование). - ISBN 978-5-534-13948-8. - URL : https://urait.ru/bcode/518006.

ОИ5. Сафиуллина Л.Х. Информационная безопасность. Практические аспекты: учебник для вузов / Л.Х. Сафиуллина, А.Р. Касимова, Я.С. Рябов, А.М. Садыков, В.А. Богомолов. - Санкт-Петербург : Интермедия, 2021. - 240 с. - ISBN 978-5-4383-0205-6. - URL: https://ibooks.ru/bookshelf/374959/reading. - Текст: электронный.

ОИ6. Сычев Ю.Н. Защита информации и информационная безопасность : учебное пособие. — (Среднее профессиональное образование) / Ю.Н. Сычев. - Москва : Инфра-М, 2021. - 201 с. - ISBN 978-5-16-109176-0. - URL: https://ibooks.ru/bookshelf/373406/reading. - Текст: электронный.

Дополнительные источники

Для преподавателей:

ДИ1. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. - 3-е изд. - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 424 с. - ISBN 978-5-4497-0336-1. - Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. - URL: https://profspo.ru/books/89451. - Режим доступа: для авторизир. пользователей.

Для студентов:

ДИ1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. - Москва : Издательство Юрайт, 2023. - 325 с. - (Профессиональное образование). - ISBN 978-5-534-00843-2. - URL : https://urait.ru/bcode/512861

ДИ2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - Москва : Издательство Юрайт, 2023. - 473 с. - (Высшее образование). - ISBN 978-5-534-12474-3. - URL : https://urait.ru/bcode/511138

ДИ3.Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Издательство Юрайт, 2023. - 349 с. - (Высшее образование). - ISBN 978-5-534-02883-6. - URL : https://urait.ru/bcode/511890.

ДИ4. Родичев Ю,А. Информационная безопасность. Национальные стандарты Российской Федерации. Учебное пособие. 3-е изд. — (Серия «Учебник для вузов»). - Санкт-Петербург : Питер, 2023. - 384 с. - ISBN 978-5-4461-2112-0. - URL: https://ibooks.ru/bookshelf/390206/reading. - Текст: электронный.

ДИ5. Родичев Ю, А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. / Ю.А. Родичев. - Санкт-Петербург : Питер, 2021. - 272 с. - ISBN 978-5-4461-9992-1. - URL: https://ibooks.ru/bookshelf/377372/reading. - Текст: электронный.

Интернет-ресурсы:

1. Источники отечественных и зарубежных нормативных документов:

1.1. http://www.etsi.org/

1.2. http://www.itu.int/

1.3. http://www.allcomponents.ru/

2. Специализированные сайты для поиска документации по электронным компонентам (datasheet):

2.1. http://www.okdatasheet.com/

2.2 http://www.allcomponents.ru/

3. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]: официальный сайт. - Режим доступа: http:// https://digital.gov.ru/ru/ /, свободный.

4. Сайт Федеральной службы безопасности России (ФСБ России) [Электронный ресурс]. - Режим доступа: http://www.fsb.ru, свободный.

5. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс]. - Режим доступа: http://www.fstec.ru/, свободный.

6. Сайт проекта Общие критерии оценки безопасности информационных технологий [Электронный ресурс]. - Режим доступа: http://www.commoncriteriaportal.org/, свободный.

7. Comnews. Новости телекоммуникаций, вещания и ИТ [Электронный ресурс]: ежедневная Интернет-газета. - Режим доступа: http://www.comnews.ru/, свободный.

8. Открытые системы [Электронный ресурс]. - Режим доступа: http://www.osp.ru/, свободный.

9. Сети и системы связи [Электронный ресурс]: архив журнала. - Режим доступа: http://www.ccc.ru/, свободный.

10. Системы управления, связи и безопасности [Электронный ресурс]: сетевой электронный журнал. - Режим доступа: http://sccs.intelgr.com/, свободный.

11. Современные телекоммуникации России [Электронный ресурс]: отраслевой информационно-аналитический онлайн-журнал. - Режим доступа: http://www.telecomru.ru/, свободный.

12. Электронная Россия [Электронный ресурс]: информационный сайт. - Режим доступа: http://www.elrussia.ru/, свободный.

13. Электросвязь [Электронный ресурс]: сайт журнала. - Режим доступа: http://www.elsv.ru/, свободный.

14. НПП «Гамма» [Электронный ресурс]: официальный сайт. - Режим доступа: https://nppgamma.ru/, свободный.

15. Группа компаний МАСКОМ [Электронный ресурс]: официальный сайт. - Режим доступа: https://www.mascom.ru/, свободный.

16. АО «ЦБИ-сервис» [Электронный ресурс]: официальный сайт. - Режим доступа: https://cbi-s.ru/catalog/sistemy-radiomonitoringa/, свободный.

17. НПО «Эшелон» [Электронный ресурс]: официальный сайт. - Режим доступа: https://npoechelon.ru/services/si/, свободный.

4.3. Общие требования к организации учебной практики

Учебная практика является одним из необходимых условий качественного освоения профессионального модуля ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи. Реализация программы учебной практики, происходит сосредоточенно после освоения всего профессионального модуля.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ УЧЕБНОЙ ПРАКТИКИ УП 03

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	- умение анализировать сетевую инфраструктуру; - выявление угроз и уязвимостей в сетевой инфраструктуре; - умение классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; - умение проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей; - определение возможных сетевых атак и способов несанкционированного доступа в конвергентных системах связи; - осуществление мероприятий по проведению аттестационных работ и выявлению каналов утечки; - выявление недостатков систем защиты в системах и сетях связи с использованием специализированных программных продуктов; - выполнение тестирования систем с целью определения уровня защищенности; - знание принципов построения информационно-коммуникационных сетей; - знание международных стандартов информационной безопасности для проводных и беспроводных сетей; - знание нормативно - правовых и законодательных актов в области информационной безопасности; - знание акустических и виброакустических каналов утечки информации, особенностей их возникновения, организации, выявления и закрытия; - знание технических каналов утечки информации, реализуемых в отношении объектов информатизации и технических средств предприятий связи, способов их обнаружения и закрытия; - знание способов и методов обнаружения средств съёма информации в радиоканале; - знание классификации угроз сетевой безопасности; - знание характерных особенностей сетевых атак; - знание возможных способов несанкционированного доступа к системам связи; - знание методов оценки угрозы инженерно-технического добывания информации; - знание методов аппаратурной оценки энергетических параметров побочных излучений от технических средств и систем передачи, хранения и обработки информации; - знание методов инженерного расчета размеров контролируемой зоны; - знание этапов проведения аудита информационной безопасности информационных систем и объектов информатизации.	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи	- умение разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи; - определение оптимальных способов обеспечения информационной безопасности; - выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях; - умение проводить мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры; - умение производить выбор необходимых средств криптографической защиты информации; - умение вырабатывать рекомендации для принятия решения	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03

	о модернизации системы защиты информации; - осуществление мероприятий по защите персональных данных; - знание правил проведения возможных проверок согласно нормативных документов ФСТЭК; - знание этапов определения конфиденциальности документов объекта защиты; - назначение, классификацию и принципы работы специализированного оборудования; - знание методов и способов защиты информации беспроводных логических сетей от НСД посредством протоколов WEP. WPA и WPA 2; - знание методов и средств защиты информации в телекоммуникациях от вредоносных программ; - знание технологий применения программных продуктов; - знание возможных способов, мест установки и настройки программных продуктов; - знание состава работ по комплексной защите информации значимых объектов критической информационной инфраструктуры; - знание концепции инженерно-технической защиты информации; - знание основных принципов организации и методов реализации технической защиты информации; - знание основных требований к системам криптографической защиты; - знание основных принципов организации работы по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСТЭК, ФСБ России.	
ПК 3.3 Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования	- умение осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи - использование специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи; - умение проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации; - разработка политики безопасности сетевых элементов и логических сетей; - выполнение расчета и установки специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; - установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи; - конфигурирование автоматизированных систем и информационно-коммуникационных сетей в соответствии с политикой информационной безопасности; - защита базы данных при помощи специализированных программных продуктов; - защита ресурсов инфокоммуникационных сетей и систем связи криптографическими методами; - администрирование наложенных программно-аппаратных средства защиты информации от НСД; - применение программно-аппаратных комплексов глубокого анализа трафика; применение программных средств, реализующих основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа; - знание методов и способов защиты информации, передаваемой по кабельным направляющим системам;	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03

	- знание конфигурации защищаемых сетей; - знание алгоритмов работы тестовых программ; - знание средств защиты различных операционных систем и среды передачи информации; - знание способов и методов шифрования (кодирование и декодирование) информации;	
ОК 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	-умение распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; умение составлять план действия; определять необходимые ресурсы; - владение актуальными методами работы в профессиональной и смежных сферах; реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	-быстрое определение сути задачи для поиска информации; необходимых источников информации; планирование процесса поиска; структурирование получаемой информации; оценивание практической значимости результатов поиска; применение средств информационных технологий для решения профессиональных задач; использование современного программного обеспечения; различных цифровых средств для решения профессиональных задач;	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03
ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	- работа в рамках актуальной нормативно-правовой документации; - применение современной научной профессиональной терминологии; - определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности;	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03
ОК 04 Эффективно взаимодействовать и работать в коллективе и команде	- организация работы коллектива и команды; - взаимодействие с коллегами, руководством, клиентами в ходе профессиональной деятельности;	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03
ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	- грамотное изложение своих мыслей и оформление документов по профессиональной тематике на государственном языке; - проявление толерантности в рабочем коллективе;	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03
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	- умение описать значимость своей специальности; - применение стандартов антикоррупционного поведения;	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03

ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- соблюдение норм экологической безопасности; - определение направлений ресурсосбережения в рамках профессиональной деятельности по специальности; - работа с соблюдением принципов бережливого производства; - организация профессиональной деятельности с учетом знаний об изменении климатических условий региона;	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03
ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- применение рациональных приемов двигательных функций в профессиональной деятельности; - умение пользоваться средствами профилактики перенапряжения характерными для данной специальности;	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	- понимание текста на базовые профессиональные темы.	- наблюдение и оценка выполнения заданий при выполнении работ по учебной практике; - комплексный дифференцированный зачет по УП 03 и ПП 03