Приложение

К ООП по специальности/профессии

10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.В.15 Практикум по защищённым виртуальным частным сетям

2025

Программу составили:

1. Кононова Наталия Владимировна

Дисциплина: ОП.В.15 Практикум по защищённым виртуальным частным сетям

Рабочая программа учебной дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утверждённым приказом Минобрнауки России от 09.12.2016 г. №1553.

Рабочая программа учебной дисциплины составлена на основании учебного плана по специальности «10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Визирование РПД для исполнения в очередном учебном году

Рассмотрено и рекомендовано на заседании кафедры Информационной безопасности

Протокол №10 от 12.05.2025

Заведующий кафедрой Кононова Наталия Владимировна

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.В.15 Практикум по защищённым виртуальным частным сетям

(наименование дисциплины)

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина ОП.В.15 Практикум по защищённым виртуальным частным сетям является обязательной частью обязательной частью цикла основной образовательной программы в соответствии ФГОС «10.02.05 Обеспечение информационной безопасности автоматизированных систем»по специальности . Особое значение дисциплина имеет при формировании и развитии общих компетенций (ОК), профессиональных компетенций (ПК):

1. ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа

1.2. Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ОК, ПК	Умения	Знания
ПК 2.4.	Разрабатывать средства и системы защиты сетей электросвязи от несанкционированного доступа, а также защищённых телекоммуникационных систем	

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объём учебной дисциплины и виды учебной дисциплины

Вид учебной работы	**Объём в часах**
Часы на контроль	6
Лабораторные занятия	14
Лекционные занятия	26
Практические занятия	6
Практическая подготовка	30
Общий объём образовательной программы учебной дисциплины, в том числе в форме практической подготовки	82
Форма(-ы) контроля: Экзамен	

2.2. Тематический план и содержание учебной дисциплины ОП.В.15 Практикум по защищённым виртуальным частным сетям

Наименование разделов и тем		Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 1 Современные технологии в профессиональной сфере	Содержание учебного материала				ПК 2.4.
	1	**Лекционные занятия №1** Специфичные требования охраны труда, техники безопасности и окружающей среды по компетенции	2	1	
Тема 2 Основы цифровой гигиены	Содержание учебного материала				ПК 2.4.
	1	**Практические занятия №1** Цифровая гигиена. Виды киберугроз. Внешние и внутренние интернет угрозы. Коммуникационные и технологические интернет угрозы.	2	2	
	2	**Практическая подготовка №1** Правила безопасного поведения в сети Интернет. Размещение и использование персональных и личных данных.	2	2	
	3	**Практические занятия №2** Безопасные пароли. Настройки приватности в социальных сетях. Резервное копирование.	4	2	
	4	**Лабораторные занятия №1** Средства шифрования данных. Средства блокирования нежелательного контента.	4	2	
	5	**Лабораторные занятия №2** Программы защиты от вредоносного программного кода. Программы родительского контроля.	4	2	
Тема 3 Современные технологии VPN. Система защиты информации ViPNet.	Содержание учебного материала				ПК 2.4.
	1	**Лекционные занятия №2** Основы защиты информации	4	1	
	2	**Лекционные занятия №3** Системы, методы и средства защиты	4	1	
	3	**Лекционные занятия №4** Правовые основы. Организационные меры по защите информации	4	1	
	4	**Лекционные занятия №5** Ключевые алгоритмы и системы	2	1	
	5	**Лабораторные занятия №3** Система защиты информации ViPNet.	2	2	
	6	**Лабораторные занятия №4** Компоненты управления сети ViPNet	2	2	
	7	**Лабораторные занятия №5** Клиентские продукты ViPNet	2	2	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объём в часах	Уровень освоения	Коды компетенций, формированию которых способствует элемент программы
Тема 4 Система VPN ViPNet. Особенности криптосистемы и ключевой структуры. Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелируемые ресурсы	Содержание учебного материала			ПК 2.4.
	1 **Лекционные занятия №6** Введение в технологию ViPNet	2	1	
	2 **Лекционные занятия №7** Современные технологии VPN.	2	1	
	3 **Лекционные занятия №8** Система защиты информации ViPNet.	2	1	
	4 **Лекционные занятия №9** Компоненты управления сети ViPNet	2	1	
	5 **Лекционные занятия №10** Серверные продукты ViPNet	2	1	
	6 **Практическая подготовка №2** Основы инфраструктуры открытых ключей.	2	2	
	7 **Практическая подготовка №3** Ключевая структура сети ViPNet. формирование и управление ключевой системой	6	2	
	8 **Практическая подготовка №4** Цифровые ключи и сертификаты.	6	2	
	9 **Практическая подготовка №5** Ключевая структура сети ViPNet. формирование и управление ключевой системой	4	2	
Тема 5 Технологии анализа и защиты сетевого трафика. Организация межсетевого взаимодействия и туннелируемые ресурсы	Содержание учебного материала			ПК 2.4.
	1 **Практическая подготовка №6** Технологии анализа и защиты сетевого трафика.	4	2	
	2 **Практическая подготовка №7** Технологии анализа и защиты сетевого трафика.	4	2	
	3 **Практическая подготовка №8** Организация межсетевого взаимодействия и туннелируемые ресурсы	2	2	
Тема 6 Промежуточный контроль	Содержание учебного материала			ПК 2.4.
	1 **Часы на контроль** Промежуточная аттестация	6	2	
	Всего	82		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (ознакомление с ранее изученными объектами, свойствами);

2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие помещения:

Лаборатория информатики и информационных технологий:

1. Проектор (1 шт.)
2. Системный блок (16 шт.)
3. Монитор (16 шт.)
4. Клавиатура (16 шт.)
5. Компьютерная мышь (16 шт.)

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные издания

1. 1. Авксентьев, А. А. Сети и системы связи : учебное пособие / А. А. Авксентьев. - 2-е изд., перераб. и доп. - Москва ; Вологда : Инфра-Инженерия, 2024. - 336 с. - ISBN 978-5-9729-1588-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2171009

3.2.2. Дополнительные источники

1. 1. Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации") Режим доступа:
2. http://www.consultant.ru/document/cons_doc_LAW_208191/
3. 2. Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации") Режим доступа:
4. http://www.consultant.ru/document/cons_doc_LAW_191669/
5. 3. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/
6. 4. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. Режим доступа: http://gostexpert.ru/gost/gost-27002-2012
7. 5. Методические указания для проведения лабораторных работ по защите

информации для студентов специальностей "Компьютерная безопасность", «Математическое обеспечение и администрирование информационных
8. систем", "Инфокоммуникационные технологии и системы связи", «Системный анализ и управление» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54 с. Режим доступа http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf.

3.2.3. Интернет-ресурсы

1. Электронно-библиотечная система Znanium.com
2. Электронно-библиотечная система BOOK.RU

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

4.1. Образовательные результаты освоения образовательной программы учебной дисциплины, подлежащие проверке

Результаты обучения	Критерии оценки	Методы оценки
Умение		
Разрабатывать средства и системы защиты сетей электросвязи от несанкционированного доступа, а также защищённых телекоммуникационных систем	владеет разработкой предложений и практической реализацией элементов, средств и систем защиты сетей от НСД, а также защищённых телекоммуникационных систем, включая разработку программного обеспечения	Тестирование, выполнение практических работ

4.2. Матрица соответствия контрольно-оценочных средств образовательным результатам учебной дисциплины

Результаты обучения	Коды компетенций	Фонды оценочных средств
Умение		
Разрабатывать средства и системы защиты сетей электросвязи от несанкционированного доступа, а также защищённых телекоммуникационных систем	ПК 2.4.	Вопросы на экзамен №1-50

Вопросы к практическому занятию указаны в методических указаниях к практическим занятиямпо дисциплине Практикум по защищённым виртуальным частным сетям для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025 Вопросы к практической подготовке указаны в методических указаниях к практической подготовкепо дисциплине Практикум по защищённым виртуальным частным сетям для обучающихся специальности "Обеспечение информационной безопасности автоматизированных систем". Ставрополь, 2025