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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СМОЛЕНСК
Сертификат: 79B4BC513DB39C55CBF2E803D8E72C94
Владелец: Овчинникова Ирина Александровна
Действителен: с 13.02.2025 до 09.05.2026

УТВЕРЖДАЮ
Зам.директора по учебной работе
_____ И. А. Овчинникова
«_14_» ____05____ 2025г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОБЩЕПРОФЕССИОНАЛЬНОГО ЦИКЛА ОП.13 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

среднего профессионального образования

для специальности
11.02.15 Инфокоммуникационные сети и системы связи

Смоленск, 2025г.

РАССМОТРЕНО
на заседании методической комиссии
компьютерных сетей и администрирования

Председатель _____ Ряска О.Г.
Протокол № 11 от «14» 05. 2025г.

СОГЛАСОВАНО
Начальник отдела эксплуатации и внедрения
информационных систем
СОГАУ «Центр информационных технологий»

_____ Я.А.Комиссаров
«14» 05 2025 г.

СОГЛАСОВАНО

Методист _____ Ряска О.Г.

«14» 05 2025 г.

Составитель: Шаманова О.О. – преподаватель высшей квалификационной категории СКТ(ф)СПбГУТ

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утвержденного приказом Министерства просвещения РФ № 675 от 05.08.2022 г. (ред. от 03.07.2024),
с учетом примерной основной образовательной программы по специальности 11.02.15 «Инфокоммуникационные сети и системы связи», разработанной Федеральным учебно-методическим объединением в системе среднего профессионального образования по укрупненным группам профессий, специальностей 11.00.00 Электроника, радиотехника и системы связи.

СОДЕРЖАНИЕ

1. Общая характеристика рабочей программы дисциплины
ОП.13 Основы информационной безопасности

1.1 Место дисциплины в структуре основной профессиональной образовательной программы: дисциплина относится к общепрофессиональному циклу.

1.2. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Код ПК, ОК	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 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.

Обязательная часть – не предусмотрено

Вариативная часть

С целью удовлетворения запросов рынка труда и обеспечения конкурентоспособности выпускника, студент должен:

Умения	У1 - классифицировать защищаемую информацию по видам тайны и степеням секретности; У2 - классифицировать основные угрозы безопасности информации; У3 - обеспечивать антивирусную защиту; У4 – использовать типовые криптографические средства и методы защиты информации.
Знания	З1 - сущность и понятие информационной безопасности, характеристику ее составляющих; З2 - основные угрозы и риски безопасности информации; З3 - основные понятия криптографии, типовые криптографические алгоритмы; З4 - способы и методы шифрования информации; З5 – биометрические технологии; З6 - средства и способы обеспечения информационной безопасности.

2. Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Виды работы	Объем часов		
	Обязательная часть	Вариативная часть	Всего
Максимальная учебная нагрузка (всего)	-	58	**58**
Обязательная аудиторная учебная нагрузка (всего)	-	50	**50***
в том числе:			
теоретическое обучение	-	28	30*
практические занятия	-	20	28
Самостоятельная работа студента в том числе: создание докладов, сообщений. Составление конспекта. Работа с ПК и Интернет-ресурсами.	-	8	**8**
Промежуточная аттестация - 4 семестр комплексный дифференцированный зачет	-	2	**2**

*Промежуточная аттестация - комплексный дифференцированный зачет
по ОП.09 Информационные технологии с ОП.13 Основы информационной безопасности проводится за счет часов лекционной нагрузки

2.2. Тематический план и содержание дисциплины ОП.13 Основы информационной безопасности

Тематический план дисциплины

Темы	**Код ПК**	**Всего *часов***		**Объём времени, отведенный на дисциплину**							
				Обязательная аудиторная учебная нагрузка студента, *часов*						Самостоятельная работа студента, *часов*	
				Всего		В том числе				Всего	
						теоретическое обучение		Лаборат. работы и практич. занятия			
		Обяз. ч	Вар. ч	Обяз. ч.	Вар. ч.	Обяз. ч.	Вар. ч.	Обяз. ч.	Вар. ч.	Обяз. ч.	Вар. ч.
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***
Тема 1. Основы информационной безопасности	ПК 3.1. ПК 3.2.	-	18	-	14	-	10	-	4	-	4
Тема 2. Средства защиты информации	ПК 3.1. ПК 3.2.	-	38	-	34	-	18	-	16	-	4
Промежуточная аттестация		-	2	-	2	-	2	-	-	-	-
Всего		**-**	**58**	**-**	**50**	**-**	**30**	**-**	**20**	**--**	**8**

Содержание дисциплины

Наименование разделов	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа студентов	Объем часов	
		Очная форма обучения	
		Обязательная часть	Вариативная часть
1	2	3	4
Тема 1. Основы информационной безопасности	1.1. Понятие информационной безопасности, характеристика ее составляющих. Целостность, доступность и конфиденциальность информации	-	2
	1.2. Система формирования режима информационной безопасности	-	2
	1.3. Нормативно-правовые основы информационной безопасности в РФ. Виды тайн и степени конфиденциальности	-	2
	1.4. Понятие угрозы информационной безопасности. Классификация угроз информационной безопасности	-	2
	1.5. Понятие уязвимости информации и формы ее проявления	-	1
	1.6. Управление рисками. Основные понятия.	-	1
	Практические занятия		
	ПЗ №1 Классификация защищаемой информации по видам тайны и степеням конфиденциальности	-	2
	ПЗ №2 Классификация защищаемой информации по форме проявления уязвимости и угрозе	-	2
	Самостоятельная работа студентов: создание докладов, сообщений. Составление таблицы сравнительных характеристик. Выполнение расчетных заданий. Составление конспекта. Работа с ПК и Интернет-ресурсами.	-	4
Тема 2. Средства защиты информации	2.1. Компьютерные вирусы как угроза информационной безопасности. Классификация вирусов.	-	2
	2.2. Жизненный цикл компьютерного вируса. Основные каналы распространения вирусов.	-	2
	2.3. Антивирусные программы и комплексы. Классификация	-	2
	2.4. Понятие аутентификации. Методы аутентификации. Аутентификация, авторизация и администрирование действий пользователей	-	2
	2.5. Биометрические системы защиты информации.	-	2
	2.6. Понятие идентификации. Методы идентификации	-	2
	2.7. Принципы криптографической защита информации. Основные понятия. Классификация	-	2
	2.8. Хеширование данных	-	2

	2.9. Компьютерная преступность и компьютерная безопасность	-	2
	Практические занятия		
	ПЗ №3 Применение антивирусной защиты в информационных системах	-	2
	ПЗ №4 Сравнение биометрических технологий	-	2
	ПЗ №5 Защита информации с использованием криптографических шифров	-	6
	ПЗ №6 Использование хеш-функций для обеспечения безопасности информации	-	4
	ПЗ №7 Защита конфиденциальной информации на рабочих местах пользователей ПК	-	2
	Самостоятельная работа студентов создание докладов, сообщений. Составление таблицы сравнительных характеристик. Выполнение расчетных заданий. Составление конспекта. Работа с ПК и Интернет-ресурсами.	-	4
Комплексный дифференцированный зачет с ОП.09 Информационные технологии		-	2
	Всего:	**-**	**58**

3. Условия реализации рабочей программы дисциплины

3.1. Материально – техническое обеспечение

Обучение по программе дисциплины осуществляется в лаборатории информационной безопасности телекоммуникационных систем:

Всего ПК – 14 шт.

- 13 х Системный блок в сборе (2022 г.в., Процессор AMD Ryzen 4600G 3.70 ГГц (6 ядер / 12 потоков), Оперативная память DDR4 32 Гб, Накопитель SSD NVMe 500 Гб, Накопитель SSD SATA 1000 Гб, Монитор 1920x1080 24"")
- 1 х Системный блок в сборе (2022 г.в., Процессор AMD Ryzen 4600G 3.70 ГГц (6 ядер / 12 потоков), Оперативная память DDR4 32 Гб, Накопитель SSD NVMe 500 Гб, Накопитель SSD SATA 1000 Гб, Монитор 1920x1080 24"")
- МФУ HP LaserJet M1132MFP (2011 г.в.)
- Проектор ViewSonic PA503X DLP 1024x768, 3600 лм (2023 г.в.)

3.2. Информационное обеспечение обучения

Основные источники:

ОИ 1. Баранова, Е. К. Основы информационней безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА-М, 2022. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1860126

ОИ 2. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — 2-е изд., доп. — Москва : ИНФРА-М, 2023. — 216 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016719-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1900721

ОИ 3. Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. - Москва ; Вологда : Инфра-Инженерия, 2022. - 104 с. - ISBN 978-5-9729-0864-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1902587

ОИ 4. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с. — ISBN 978-5-507-48149-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/341267

ОИ 5. Пугин, В. В. Основы информационной безопасности : методические указания / В. В. Пугин. — Самара : ПГУТИ, 2021. — 39 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/301181

ОИ 6. Поляков, Е. А. Основы информационной безопасности : учебное пособие / Е. А. Поляков. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2021. — 71 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/282890

Дополнительные источники:

ДИ 1. Гродзенский Я. С. Информационная безопасность : учебное пособие / Я.С. Гродзенский. - Москва : Проспект, 2020. - 144 с. - ISBN 978-5-9988-0845-6. - URL: https://ibooks.ru/bookshelf/373686/reading

ДИ 2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. - Москва : Форум, 2021. - 416 с. - ISBN 978-5-8199-0754-2. - URL: https://ibooks.ru/bookshelf/361273/reading

Интернет ресурсы и источники:

1. Электронно-библиотечная система издательства «Лань» [Электронный ресурс]. – Режим доступа: e.lanbook.com
2. Электронно-библиотечная система «Ibooks.ru» [Электронный ресурс]. – Режим доступа:

ibooks.ru
3. Электронно-библиотечная система издательства «Profобразование» [Электронный ресурс]. – Режим доступа: profspo.ru
4. Электронно-библиотечная система «Znanium» [Электронный ресурс]. – Режим доступа: znanium.com

4. Контроль и оценка результатов освоения дисциплины

Результаты обучения	*Критерии оценки*	*Формы и методы оценки*
У1 - классифицировать защищаемую информацию по видам тайны и степеням секретности; У2 - классифицировать основные угрозы безопасности информации; У3 - обеспечивать антивирусную защиту; У4 – использовать типовые криптографические средства и методы защиты информации.	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Формы и методы контроля и оценки: • Компьютерное тестирование. • Самостоятельная работа. • Наблюдение за выполнением практического занятия. • Защита практического занятия. • Промежуточная аттестация (комплексный дифференцированный зачет в виде тестирования)
З1 - сущность и понятие информационной безопасности, характеристику ее составляющих; З2 - основные угрозы и риски безопасности информации; З3 - основные понятия криптографии, типовые криптографические алгоритмы; З4 - способы и методы шифрования информации; З5 – биометрические технологии; З6 - средства и способы обеспечения информационной безопасности.		• Подготовка и выступление с докладом, сообщением, презентацией. • Решение ситуационной задачи. • Текущий контроль (проверочные работы, тесты) • Промежуточная аттестация (комплексный дифференцированный зачет в виде тестирования)

Конкретизация результатов освоения дисциплины

ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	
Уметь: У1 - классифицировать защищаемую информацию по видам тайны и степеням секретности; У2 - классифицировать основные угрозы безопасности информации; У3 - обеспечивать антивирусную защиту; У4 – использовать типовые криптографические средства и методы защиты информации.	Тематика практических занятий: ПЗ №1 Классификация защищаемой информации по видам тайны и степеням конфиденциальности ПЗ №2 Классификация защищаемой информации по форме проявления уязвимости и угрозе ПЗ №3 Применение антивирусной защиты в информационных системах ПЗ №4 Сравнение биометрических технологий ПЗ №5 Защита информации с использованием криптографических шифров ПЗ №6 Использование хеш-функций для обеспечения безопасности информации ПЗ №7 Защита конфиденциальной информации на рабочих местах пользователей ПК
Знать: З1 - сущность и понятие информационной безопасности, характеристику ее составляющих; З2 - основные угрозы и риски безопасности информации; З3 - основные понятия криптографии, типовые криптографические алгоритмы; З4 - способы и методы шифрования информации; З5 – биометрические технологии; З6 - средства и способы обеспечения информационной безопасности.	Перечень тем: 1.1. Понятие информационной безопасности, характеристика ее составляющих. Целостность, доступность и конфиденциальность информации 1.2. Система формирования режима информационной безопасности. 1.3. Нормативно-правовые основы информационной безопасности в РФ. Виды тайн и степени конфиденциальности. 1.4. Понятие угрозы информационной безопасности. Классификация угроз информационной безопасности 1.5. Понятие уязвимости информации и формы ее проявления 1.6. Управление рисками. Основные понятия. 2.1. Компьютерные вирусы как угроза информационной безопасности. Классификация вирусов. 2.2. Жизненный цикл компьютерного вируса. Основные каналы распространения вирусов. 2.3. Антивирусные программы и комплексы. Классификация 2.4. Понятие аутентификации. Методы аутентификации. Аутентификация, авторизация и администрирование действий пользователей 2.5. Биометрические системы защиты информации. 2.6. Понятие идентификации. Методы идентификации 2.7. Принципы криптографической защита информации. Основные понятия. Классификация 2.8. Хеширование данных 2.9. Компьютерная преступность и компьютерная безопасность
Самостоятельная работа	Тематика самостоятельной работы: Создание докладов, сообщений. Составление таблицы сравнительных характеристик. Выполнение расчетных заданий. Составление конспекта. Работа с ПК и Интернет-ресурсами.
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи	
Уметь: У1- обрабатывать тек У1 - классифицировать	Тематика практических занятий: ПЗ №1 Классификация защищаемой информации по видам тайны и степеням конфиденциальности

защищаемую информацию по видам тайны и степеням секретности; У2 - классифицировать основные угрозы безопасности информации; У3 - обеспечивать антивирусную защиту; У4 – использовать типовые криптографические средства и методы защиты информации.	ПЗ №2 Классификация защищаемой информации по форме проявления уязвимости и угрозе ПЗ №3 Применение антивирусной защиты в информационных системах ПЗ №4 Сравнение биометрических технологий ПЗ №5 Защита информации с использованием криптографических шифров ПЗ №6 Использование хеш-функций для обеспечения безопасности информации ПЗ №7 Защита конфиденциальной информации на рабочих местах пользователей ПК
Знать: З1 - сущность и понятие информационной безопасности, характеристику ее составляющих; З2 - основные угрозы и риски безопасности информации; З3 - основные понятия криптографии, типовые криптографические алгоритмы; З4 - способы и методы шифрования информации; З5 – биометрические технологии; З6 - средства и способы обеспечения информационной безопасности.	Перечень тем: 1.1. Понятие информационной безопасности, характеристика ее составляющих. Целостность, доступность и конфиденциальность информации 1.2. Система формирования режима информационной безопасности. 1.3. Нормативно-правовые основы информационной безопасности в РФ. Виды тайн и степени конфиденциальности. 1.4. Понятие угрозы информационной безопасности. Классификация угроз информационной безопасности 1.5. Понятие уязвимости информации и формы ее проявления 1.6. Управление рисками. Основные понятия. 2.1. Компьютерные вирусы как угроза информационной безопасности. Классификация вирусов. 2.2. Жизненный цикл компьютерного вируса. Основные каналы распространения вирусов. 2.3. Антивирусные программы и комплексы. Классификация 2.4. Понятие аутентификации. Методы аутентификации. Аутентификация, авторизация и администрирование действий пользователей 2.5. Биометрические системы защиты информации. 2.6. Понятие идентификации. Методы идентификации 2.7. Принципы криптографической защита информации. Основные понятия. Классификация 2.8. Хеширование данных 2.9. Компьютерная преступность и компьютерная безопасность
Самостоятельная работа	Тематика самостоятельной работы: Создание докладов, сообщений. Составление таблицы сравнительных характеристик. Выполнение расчетных заданий. Составление конспекта. Работа с ПК и Интернет-ресурсами.

Приложение 2

Технологии формирования ОК

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.	• выбор и применение методов и способов решения профессиональных задач в области информационных технологий; • оценка эффективности и качества выполнения профессиональных задач.	**Текущий контроль в форме:** - наблюдения во время выполнения заданий; - защиты практических занятий; - защиты рефератов. - компьютерного тестирования.
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	• эффективный поиск необходимой информации; • использование различных источников, включая электронные.	**Текущий контроль в виде:** проверки докладов, рефератов, презентаций, подготовленных с использованием электронных источников.

Лист изменений рабочей программы

Содержание изменения, страница рабочей программы	Дата и номер протокола заседания МК	Основание для внесения изменения
1.		
2.		
3.		