

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

 И.А. Овчинникова

« 14 » 25 2025 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С
ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-
АППАРАТНЫХ, В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ
ЗАЩИТЫ

среднего профессионального образования

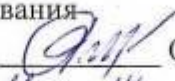
для специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных
систем

г. Смоленск, 2025 г.

РАССМОТРЕНО

на заседании методической комиссии
информационной безопасности и сетевого
администрирования

Председатель  О.Г. Ряска

Протокол № 11 от «14» 05 2025 г.

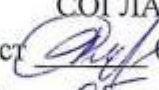
СОГЛАСОВАНО

Инженер ООО «Арсенал 67»

 Р.Н. Михайлов

«14» 05 2025 г.

СОГЛАСОВАНО

Методист  О.Г. Ряска

«14» 05 2025 г.

Составитель: Королев Е.В. – преподаватель первой квалификационной категории
СКТ(ф) СПбГУТ.

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки РФ от 09.12.2016 г. №1551 (ред. от 03.07.2024), а также на основании примерной основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, разработанной ФУМО в системе СПО по УГС 10.00.00 «Информационная безопасность».

СОДЕРЖАНИЕ

1. Общая характеристика рабочей программы профессионального модуля ПМ. 02 Защита информации в информационно - телекоммуникационных системах и сетях с использованием программных и программно- аппаратных, в том числе криптографических средств защиты	4
2. Структура и содержание профессионального модуля	7
3. Условия реализации программы профессионального модуля	9
4. Контроль и оценка результатов освоения профессионального модуля	10

Приложение 1

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля (далее – ПМ) ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты, студент должен освоить такой основной вид деятельности, как защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты, и овладеть следующими общими и профессиональными компетенциями:

Код	Наименование видов деятельности и 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 правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде.
ВД 2.	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты
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 оборудовании информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе 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 предъявляемыми требованиями.

В результате освоения профессионального модуля в обязательной части студент должен

Иметь практический опыт	в ПО 1 - установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей; в ПО 2 - поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; в ПО 3 - защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями
уметь	У 1 - выявлять и оценивать угрозы безопасности информации в ИТКС; У 2 - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; У 3 - проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; У 4 - проводить конфигурирование программных и программно-аппаратных, в

	том числе криптографических средств защиты информации; У 5 - проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; У 6 - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; У 7 - проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации.
знать	З 1 - возможные угрозы безопасности информации в ИТКС; З 2 - способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее; З 3 - типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; З 4 - криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; З 5 - порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; З 6 - организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; З 7 - порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации.

В вариативной части

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

Иметь практический опыт	в ПО 4 - определения необходимых средств криптографической защиты информации;
уметь	У 8 - определять рациональные методы и средства защиты на объектах и оценивать их эффективность; У 9 - пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
знать	З 8 - типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; З 9 - основные протоколы идентификации и аутентификации в телекоммуникационных системах; З 10 - особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;

2. Структура и содержание профессионального модуля

2.1. Структура ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

Наименования разделов профессионального модуля	Коды профессиональных общих компетенций	Суммарный объем нагрузки, час.	Занятия во взаимодействии с преподавателем, час							Самостоят. работа
			Обучение по МДК			Практики				
			Лекции	Лабораторных и практических занятий	Курсовых работ (проектов)	Учебная	Производственная	Промежуточная аттестация	Консультация	
1	2	3	4	5	6	7	8	9	10	11
Раздел 1. МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	ПК 2.1-ПК 2.3 ОК 01-04	292	140	66	30	-	-	-	-	56
Раздел 2. МДК 02.02 Криптографическая защита информации	ПК 2.1-ПК 2.3 ОК 01-04	178	104	44	-	-	-	6	2	22
Учебная практика	ПК 2.1-ПК 2.3 ОК 01-04	108				108	-	-	-	-
Производственная практика	ПК 2.1-ПК 2.3 ОК 01-04	180					180	-	-	-
Экзамен квалификационный	ПК 2.1-ПК 2.3 ОК 01-04	18						18		
Всего:		776	244	110	30	108	180	24	2	78

2.2. Тематический план и содержание профессионального модуля (ПМ)

Содержание учебного материала, лабораторные занятия и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект), виды учебной практики и виды производственной практики прилагаются отдельными документами:

1. Рабочая программа по МДК 02.01 Защита информации в информационно телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты.
2. Рабочая программа по МДК 02.02 Криптографическая защита информации.
3. Рабочая программа учебной практики УП.02.
4. Рабочая программа производственной практики ПП.02.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНЫХ И ПРОГРАММНО-АППАРАТНЫХ, В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Лаборатория программных и программно-аппаратных средств защиты информации (Ауд.315)

Типовой комплект учебного оборудования «Сетевая безопасность» - 1 шт.;

Виртуальный тренажёр «Программные средства криптографии» - 1 шт.;

Учебно-практический стенд «Системы контроля и управления доступом» – 1 шт.;

Учебный стенд «Программные средства криптографии» – 1 шт.;

Набор программного обеспечения для развёртывания стенда «Программные средства криптографии» - 1 шт.;

Учебный стенд «Системы доверенной загрузки» – 1 шт.;

Учебный стенд «Программные средства защиты информации от несанкционированного доступа» – 1 шт.

Системный блок в комплекте с клавиатурой и мышью: процессор 6 ядер/12 потоков, оперативная память 16 Гб, твердотельный накопитель 1 480 Гб, твердотельный накопитель 2 1000 Гб – 13 шт.;

Локальная сеть с выходом в Интернет топологии «звезда», 1 Гб/сек.

Свободные дистрибутивы операционных систем Linux (Ubuntu, Debian, CentOS).

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Электронные издания (электронные ресурсы)

ОИ.1 Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1215714>

ОИ.2 Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/176563>

ОИ.3 Маршаков, Д. В. Методы и средства криптографической защиты информации. Практический курс : учебное пособие / Д.В. Маршаков, Д.В. Фахти. — Москва : ИНФРА-М, 2022. — 76 с. — (Высшее образование). - ISBN 978-5-16-110842-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1891129>

ОИ.4 Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189341>

ОИ5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1843022>

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 «IPRbook» [Электронный ресурс]. – Режим доступа: iprbookshop.ru
4. Электронно-библиотечная система издательства « [Электронный ресурс]. – Режим доступа: profspo.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
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 оборудовании информационно-телекоммуникационных систем и сетей.	- выявлять и оценивать угрозы безопасности информации в 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;	Экзамен квалификационный в форме собеседования - экспертное наблюдение
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	- 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;	Экзамен квалификационный в форме собеседования - экспертное наблюдение
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 предъявляемыми требованиями.	- 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;	Экзамен квалификационный в форме собеседования - экспертное наблюдение

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;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экзамен квалификационный в форме собеседования - экспертное наблюдение
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные 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 правовой и финансовой грамотности в различных жизненных ситуациях.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	

Лист изменений

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