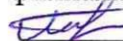


Смоленский колледж телекоммуникаций (филиал)
Федерального государственного бюджетного образовательного учреждения
высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

СОГЛАСОВАНО

Руководитель направления Управления

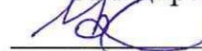
безопасности Смоленского
филиала ПАО "Ростелеком"

 В.А. Петров

«_31_»__08____2023г.

УТВЕРЖДАЮ

Зам. директора по УР

 И.В. Иванешко

«_31_»__08____2023г.

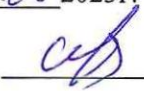
РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА

«МДК 02.02 Криптографическая защита информации»

основной образовательной программы подготовки специалистов среднего звена
по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных
систем

Смоленск, 2023 г.

Рассмотрено
На заседании методической
комиссии компьютерных сетей
и администрирования
Протокол № 1 31.08 2023г.

Председатель МК  О.С. Скряго

Составители: Скряго О.С. – преподаватель высшей квалификационной категории
СКТ(ф)СПбГУТ

Рецензенты:

Внутренний рецензент:

Шаманова О.О., преподаватель СКТ(ф)СПбГУТ высшей квалификационной категории.

Внешний рецензент:

Рецензент Ефремов А.А., ведущий специалист-эксперт отдела по защите информации ГУ-ОПФ по Смоленской области

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 09.12.2016г. №1551 (ред.17.12.2020), 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 МЕЖДИСЦИПЛИНАРНОГО КУРСА	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА.....	6
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА.....	12

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

1.1. Цель и планируемые результаты освоения междисциплинарного курса

Рабочая программа междисциплинарного курса (далее программа МДК) МДК 02.02 Криптографическая защита информации – является частью 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 подготовки специалистов среднего звена в соответствии ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем и в части освоения основного вида деятельности (ВД): Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты и соответствующих общих и профессиональных компетенций (ПК):

1.1.1. Перечень общих компетенций

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
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 оборудование 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.

1.1.3. В результате освоения междисциплинарного курса 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; ПО2 - поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; ПО3 - 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	У1 -выявлять и оценивать угрозы безопасности информации в ИТКС; У3 - проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; У4- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации; У5 - проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; У6-проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; У7- проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации.
знать	31- возможные угрозы безопасности информации в ИТКС; 32 - способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее; 33 - типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; 34 - криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; 35 - порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; 36 - организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; 37 - порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации.

Вариативная часть

С целью удовлетворения запросов рынка труда и обеспечения конкурентоспособности выпускника, а так же с целью удовлетворения требований профессионального мастерства по стандартам WorldSkills Russia студент должен иметь практический опыт:

Иметь практический опыт в	ПО4- определения необходимых средств криптографической защиты информации;
уметь	У9 - пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
знать	38 - типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;

2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

2.1 Количество часов, отводимое на освоение междисциплинарного курса МДК 02.02 Криптографическая защита информации

Всего часов 178, из них – 128 часов – обязательная часть, 50 часов – вариативная часть, включая:

обязательной аудиторной учебной нагрузки студента – 148 часов;

самостоятельной работы студента – 22 часа;

консультация – 2 часа

Промежуточная аттестация – 6 часов экзамен (7 семестр);

Вид учебной работы	Объём в часах
Объём образовательной программы	178
в том числе:	
теоретическое обучение	104
практические занятия	24
лабораторные занятия	20
курсовое проектирование	-
консультации	2
<i>Самостоятельная работа</i>	22
Промежуточная аттестация экзамен (7 семестр)	6

2.2. Тематический план и содержание междисциплинарного курса МДК 02.02 Криптографическая защита информации

Наименование разделов междисциплинарного курса (МДК) и тем	Содержание учебного материала, лабораторные занятия и практические занятия, самостоятельная работа обучающихся, курсовой проект	Объем часов
1	2	3
ПМ.02.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты		
Раздел 2.Криптографическая защита информации		
МДК 02.02.Криптографическая защита информации		
Тема 2.1. Основы криптографических методов защиты информации	Содержание	40
	Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Криптографические методы. Шифрование. Кодирование. Стеганография. Сжатие. Математика криптографии. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Традиционные шифры перестановки. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. Традиционные шифры замены. Шифры замены. Шифры многоалфавитной замены. Частотность символов. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста . Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	30

Тема 2.2. Современные стандарты шифрования	Практические занятия	2
	ПЗ№1 Использование алгоритмов шифрования для сокрытия содержимого файла с применением OpenSSL	2
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	8
	Содержание	41
	Симметричное шифрование. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES. Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES. Российские стандарты симметричного шифрования. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. Проблема распределения ключей симметричного шифрования. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. Асимметричное шифрование. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль-Гамала. Криптосистемы на основе метода эллиптических кривых. ЭЦП. Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.	30
	Практические занятия	4
	ПЗ№2 Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа.	2
	ПЗ№3 Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	2
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	7
	Содержание	89

Тема Криптографические методы обеспечения безопасности сетевых технологий	2.3. Целостность сообщения. Случайная модель Ogaclе. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции. Электронная цифровая подпись. Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012. Установление подлинности объекта. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. Проблемы распределения открытого ключа асимметричного шифрования. Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. Электронная почта. Архитектура e-mail. PGP. S/MIME . Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети Защита информации в сетях организованных по технологии беспроводного доступа. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16. Защита информации в сетях сотовой связи. A3. A8.A5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи. Криптовалюты. Биткоин. Блокчейн-системы Ethereum. Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.	44
	Практические и лабораторные занятия	38

	ПЗ №4 Использование алгоритмов хеширования для подтверждения неизменности файла с применением OpenSSL.	2
	ПЗ№5 Создание цифровых сертификатов X.509 и преобразование их форматов с применением пакета OpenSSL.	2
	ПЗ№6 Создание центра сертификации с поддержкой списков отозванных сертификатов с применением пакета OpenSSL.	2
	ПЗ№7 Создание центра сертификации с поддержкой протокола OCSP с применением пакета OpenSSL.	2
	ПЗ№8 Применение «сетей доверия» для распространения сертификатов.	2
	ПЗ№9 Применение электронной цифровой подписи для проверки авторства и неизменности файла.	2
	ПЗ№10 Изучение каркаса обеспечения безопасности ISAKMP на примере протокола туннелирования IPSec.	2
	ПЗ№11 Безопасное хранение файлов с применением криптоконтейнеров.	2
	ПЗ№12 Создание файловой системы с поддержкой прозрачного шифрования.	2
	ЛЗ№1 Система обнаружения руткитов tripwire.	2
	ЛЗ№2 Применение stunnel для шифрования данных, передаваемых с помощью протокола telnet.	2
	ЛЗ№3 Хеширование по алгоритмам MD5, SHA-1, SHA-256, SHA-512. Оценка криптостойкости.	2
	ЛЗ№4 Перехват и расшифровка трафика. Определение типа шифрования.	2
	ЛЗ№5 Знакомство с действующим криптографическим ПО.	2
	ЛЗ№6 Обзор инструментов KaliLinux.	2
	ЛЗ№7 Стресс-тесты сети.	2
	ЛЗ№8 Анализ уязвимостей в операционных системах и серверном ПО.	2
	ЛЗ№9 Сканирование сетей. Перехват данных по сетям.	2
	ЛЗ№10 Атаки на пароли. Брутфорсинг.	2
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	7
Консультация		2
Промежуточная аттестация экзамен (5 семестр)		6
ВСЕГО		178

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

3.1. Для реализации программы междисциплинарного курса предусмотрены следующие специальное помещение:

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

Электронные издания (электронные ресурсы)

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>

ОИ.5 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:

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. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МЕЖДИСЦИПЛИНАРНОГО КУРСА**

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы 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;	Дифференцированный зачет в форме тестирования Защита отчетов по лабораторным занятиям и практическим занятиям
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	Дифференцированный зачет в форме тестирования Защита отчетов по лабораторным занятиям и практическим занятиям

	числе криптографических) средств защиты информации;	
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;	Дифференцированный зачет в форме тестирования Защита отчетов по лабораторным занятиям и практическим занятиям

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
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение и оценка на лабораторных занятиях, при выполнении работ практической подготовки по учебной и

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	производственной практикам Экзамен квалификационный
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	

Лист изменений

Содержание изменения, страница рабочей программы	Дата и номер протокола заседания МК	Основание изменения
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		

Р Е Ц Е Н З И Я
НА РАБОЧУЮ ПРОГРАММУ
МЕЖДИСЦИПЛИНАРНОГО КУРСА

МДК 02.02 Криптографическая защита информации
по специальности 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

На рецензию представлена рабочая программа междисциплинарного курса МДК 02.02 Криптографическая защита информации по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

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 09.12.2016г. №1551, 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 программы ориентировано на подготовку студентов к овладению профессиональными компетенциями:

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 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.

Промежуточная аттестация экзамен.

Рабочая программа разработана для очной формы обучения.

Рабочая программа междисциплинарного курса МДК 02.02 Криптографическая защита информации по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, заслуживает высокой оценки и рекомендуется для использования в учебном процессе.

Рецензент: _____



Шаманова О.О.

преподаватель высшей категории
СКТ(ф)СПбГУТ

Р Е Ц Е Н З И Я
НА РАБОЧУЮ ПРОГРАММУ
МЕЖДИСЦИПЛИНАРНОГО КУРСА

МДК 02.02 Криптографическая защита информации
по специальности 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

На рецензию представлена рабочая программа междисциплинарного курса МДК 02.02 Криптографическая защита информации по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем объемом 178 часов.

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 09.12.2016г. №1551.

Рабочая программа междисциплинарного курса (далее программа МДК) МДК 02.02 Криптографическая защита информации – является частью 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.

Содержание программы ориентировано на подготовку студентов к овладению профессиональными компетенциями:

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 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 рабочей программе подробно описаны темы, которые рассматриваются в рамке данного курса: основы криптографических методов защиты информации, современные стандарты шифрования, криптографические методы обеспечения безопасности сетевых технологий.

Рабочая программа междисциплинарного курса МДК 02.02 Криптографическая защита информации по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, заслуживает высокой оценки и рекомендуется для использования в учебном процессе.

Рецензент: 
эксперт отдела по защите информации ГУ-ОПФ по Смоленской области

Ефремов А.А. ведущий специалист-области