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.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СМОЛЕНСК
Сертификат: 009533997B26BB162CCCB9A17C8FD30591
Владелец: Иванешко Ирина Васильевна
Действителен: с 22.05.2023 до 14.08.2024

РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА

«МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»

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
Рецезенты:

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 ……13

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА……...14

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

1.1. Цель и планируемые результаты освоения междисциплинарного курса

Рабочая программа междисциплинарного курса (далее программа МДК) МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты» – 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; У2 -настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; 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	З1- возможные угрозы безопасности информации в ИТКС; З2 - способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее; З3 - типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; З5 - порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; З6 - организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; З7 - 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:

уметь	У8 - определять рациональные методы и средства защиты на объектах и оценивать их эффективность;
знать	З9 - основные протоколы идентификации и аутентификации в телекоммуникационных системах; З10 - особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;

2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

2.1 Количество часов, отводимое на освоение междисциплинарного курса МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

Всего часов __292___, из них – 226 часов – обязательная часть, 66 часов – вариативная часть, включая:
обязательной аудиторной учебной нагрузки студента – 236 часов;

самостоятельной работы студента – 56 часов;

Промежуточная аттестация – другие формы (5 семестр);

дифференцированный зачет (6 семестр)

Вид учебной работы	Объём в часах
Объем образовательной программы	292
в том числе:	
теоретическое обучение	140
практические занятия	30
лабораторные занятия	36
курсовое проектирование	30
консультации	-
Самостоятельная работа	56
Промежуточная аттестация другие формы (5 семестр), дифференцированный зачет (6 семестр)	

2.2. Тематический план и содержание междисциплинарного курса МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

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 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		
Тема 1.1. Обеспечение безопасности операционных систем	Содержание Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации Пароли. PIN-коды. Методы надежного составления паролей. Строгая аутентификация. Односторонняя аутентификация. Двухсторонняя аутентификация Аппаратно-программные средства идентификации и аутентификации. Учебный стенд "Системы доверенной загрузки", ПЗИ-МДЗ Настройку программного обеспечения Контролировать доступ при запуске ПК Контролировать программные и аппаратные средства защищаемой системы Организовать защиты от подбора пароля к запускаемой ОС Вести протоколирование доступа к системе Ограничение доступа к файлам и внешним источникам данных	30
	Практические занятия и лабораторные занятия	**20**

	ПЗ 1Изучение средств идентификации аутентификации операционных систем. Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя.	6
	ПЗ2 Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	2
	ЛЗ1 Доверенная загрузка ОС.	4
	ЛЗ2 Защита от несанкционированного доступа к ПК.	2
	ЛЗ3Аутентификация и разграничение доступа пользователей.	2
	ЛЗ4Механизмы контроля целостности системных файлов.	4
	ЛЗ5Протоколирование событий доступа к файлам.	2
	ЛЗ 6Контроль печати защищенных документов.	2
	ЛЗ 7 Контроль доступа к носителям информации.	2
	Самостоятельная работа студентов: составление презентации, подготовка реферата, заполнение рабочей тетради для выполнения практических занятий.	10
Тема 1.2. Технологии разграничения доступа	**Содержание**	**28**
	Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. Особенности функционирования межсетевых экранов. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Схемы защиты на базе межсетевых экранов. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. Программные средства защиты информации от несанкционированного доступа Двухфакторную аутентификацию до загрузки системы с помощью аппаратных идентификаторов. Ограничение запуска приложений. Журналирование событий безопасности.	

	Контроль аппаратной и программной целостности системы. Управление пользователями и устройствами системы. Межсетевое экранирование для ограничения доступа к удаленным ресурсам.	
	Практические и лабораторные занятия	
	ПЗ3Архивирование информации	4
	ЛЗ8Защищенный вход в систему	4
	ЛЗ9 Ограничение запуска и установки программ	4
	ЛЗ 10 Контроль утечки и каналов распространения информации	4
	ЛЗ11 Контроль аппаратной целостности	2
	ЛЗ12 Централизованное управление средствами защиты информации на оконечных устройствах	2
	ЛЗ13 Использование межсетевого экрана для защиты от несанкционированного доступа	2
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	10
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание**	
	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP. Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. VPN – решения для построения защищенных сетей. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP.	**26**

	Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом. Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	
	Практические занятия	
	ПЗ 4 Основные действия с виртуальной машиной	2
	ПЗ 5Работа с контрольными точками	4
	ПЗ 6Использование внешних устройств	4
	ПЗ 7Работа с локальным хранилищем сертификатов в ОС WINDOWS	4
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	13
Тема 1.4. Технологии обнаружения вторжений	**Содержание**	**36**
	Технология обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак. Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.	

	Практические занятия	**8**
	ПЗ 8Изучение средств обнаружения атак	4
	ПЗ9 Изучение антивирусных продуктов	4
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	13
Тема 1.5. Методы управления средствами защиты	**Содержание**	**20**
	Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. Обзор современных систем управления сетевой защитой. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.	
	Самостоятельная работа студентов: составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами	10
Курсовой проект **Тематика курсовых проектов:** 1. Модель угроз НСД на предприятии 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии 6. Построение модели нарушителя по требованиям ФСБ на предприятии 7. Модель угроз безопасности ИС персональных данных на предприятии 8. Комплексная модель защиты информации на предприятии. 9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)		30

10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 13. Проблема защиты информации в облачных хранилищах данных и ЦОДах 14. Защита сред виртуализации.	
Консультация	-
Промежуточная аттестация другие формы (5 семестр), дифференцированный зачет (6 семестр)	

Электронные издания (электронные ресурсы)

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 оборудование 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

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 «Програмные 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

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

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;	Дифференцированный зачет в форме тестирования Защита отчетов по лабораторным занятиям и практическим занятиям
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

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;	образовательной программы Экспертное наблюдение и оценка на лабораторных занятиях, при выполнении работ практической подготовки по учебной и производственной практикам Экзамен квалификационный
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	
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 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»
по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

На рецензию представлена рабочая программа междисциплинарного курса «МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты» 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 другие формы (3 семестр), дифференцированный зачет (4 семестр).

Рабочая программа разработана для очной формы обучения.

Рабочая программа междисциплинарного курса «МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты» 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 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»

по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

На рецензию представлена рабочая программа междисциплинарного курса МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем объемом 292 часа.

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.

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: обеспечение безопасности операционных систем, технологии разграничения доступа, обеспечение информационной безопасности сетей, основы технологии виртуальных защищенных сетей VPN, технологии обнаружения вторжений, методы управления средствами защиты.

Рабочая программа междисциплинарного курса «МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты» по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, заслуживает высокой оценки и рекомендуется для использования в учебном процессе.

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