МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

УТВЕРЖДАЮ
зам. директора по УМР
_____С.А. Косова
«02» 06 2023 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.04 Основы информационной безопасности

10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

г. Шатура
2023 г.

Рабочая программа учебной дисциплины разработана в соответствии Федеральным государственным образовательным стандартом (далее - ФГОС) по специальности программы подготовки специалистов среднего звена (далее ППССЗ) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (базовой подготовки).

Организация-разработчик: ГБПОУ МО «ШЭТ»

Разработчики:

Краснолобов Дмитрий Михайлович, преподаватель специальных дисциплин

ОДОБРЕНО

цикловой комиссией преподавателей специальности УГС Информатика и вычислительная техника и Информационная безопасность (09.02.06, 10.02.04)

Протокол № 11 от «01» 06 2023 г.

Председатель ЦК: _____ Е.А. Еремина

Внутренний рецензент: _____ Е.В. Лялина, методист ГБПОУ МО «ШЭТ»

СОДЕРЖАНИЕ:

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Место дисциплины в структуре основной образовательной программы

Рабочая программа учебной дисциплины ОП.04 Основы информационной безопасности является обязательной частью общепрофессионального цикла основной образовательной программы ППССЗ в соответствии с ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Особое значение дисциплина имеет при формировании и развитии общих и профессиональных компетенций для дальнейшего освоения профессиональных модулей.

При реализации программы могут применяться дистанционные образовательные технологии, электронное и сетевое обучения.

1.2. Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания:

Код ПК, ОК, ЛР	Умения	Знания
ОК 03, ОК 06, ОК 09, ОК 10, ПК 2.4 ЛР 10, ЛР 15, ЛР 17	классифицировать защищаемую информацию по видам тайны и степеням секретности; классифицировать основные угрозы безопасности информации;	сущность и понятие информационной безопасности, характеристику ее составляющих; место информационной безопасности в системе национальной безопасности страны; виды, источники и носители защищаемой информации; источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности;

2. Структура и содержание учебной дисциплины.

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем, часов
Объем образовательной программы учебной дисциплины	**58**
в том числе:	
теоретическое обучение	*28*
лабораторные работы	*20*
консультации	*2*
Промежуточная аттестация *в форме экзамена*	8

2.2. Тематический план и содержание учебной дисциплины

ОП.04 Основы информационной безопасности

Наименование разделов, тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовой проект	Объем часов	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Раздел 1 Теоретические основы информационной безопасности		**28**	
Тема 1.1. Основные понятия и задачи информационной безопасности.	**Содержание:**	**2**	ОК 3, ОК 6, ОК 9, ПК.2.4 ЛР 10,15,17
	1. Понятие информации и информационной безопасности.	**2**	
	2. Понятие «угроза информации». Понятие «риска информационной безопасности».	**2**	
Тема 1.2. Основы защиты информации.	**Содержание:**	**16**	ОК 3, ОК 6, ОК 9, ПК 2.4 ЛР 10,15,17
	1. Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности.	4	
	2. Цели и задачи защиты информации. Основные понятия в области защиты информации.	4	
	Лабораторные работы:		
	ЛР №1: Классификация защищаемой информации по видам и степеням конфиденциальности	4	
	ЛР №2: Определение объектов защиты на типовом объекте информатизации	4	
Тема 1.3. Угрозы безопасности защищаемой информации.	**Содержание:**	**8**	ОК 3, ОК 6, ОК 9, ПК.2.4 ЛР 10,15,17
	1. Понятие угрозы безопасности информации.	4	
	Лабораторные работы:		
	ЛР №3: Определение угроз объекта информатизации и их классификация	4	
Раздел 2. Методология защиты информации		**20**	
Тема 2.1. Методологические	**Содержание:**		ОК 3, ОК 6, ОК 9, ПК 2.4 ЛР 10,15,17
	1. Анализ существующих методик определения требований к защите информации.	4	

Наименование разделов, тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовой проект	Объем часов	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
подходы к защите информации			
Тема 2.2. Нормативно правовое регулирование защиты информации	**Содержание:**	8	ОК 3, ОК 6, ОК 9, ОК 10 ЛР 10,15,17
	1. Организационная структура системы защиты информации. Законодательные акты в области защиты информации.	4	
	Лабораторные работы:		
	ЛР №4: Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	4	
Тема 2.3. Защита информации в автоматизированных (информационных) системах.	**Содержание:**	8	ОК 3, ОК 6, ОК 9, ОК 10 ЛР 10,15,17
	1. Основные механизмы защиты информации. Система защиты информации.	4	
	Лабораторные работы:		
	ЛР №5: Выбор мер защиты информации для автоматизированного рабочего места	4	
Экзамен		**8**	
Консультации		**2**	
ИТОГО		**58**	

3. Условия реализации программы учебной дисциплины.

3.1. Требования к минимальному материально-техническому обеспечению:

Реализация учебной дисциплины требует наличия учебного кабинета «Основ информационной безопасности»

Оборудование учебного кабинета:

- посадочных мест по количеству обучающихся;

-стулья;

-доска классная;

- рабочее место преподавателя.

Технические средства обучения:

- компьютер с лицензионно-программным обеспечением и мультимедийный проектор;

-экран проекционный.

Учебные наглядные пособия:

- комплекты учебно-наглядных пособий по дисциплине.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

Основные источники (ОИ):

№ п/п	Наименование	Автор	Издательство, год издания
[1]	*Основы информационной безопасности*	*Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А.*	*Академия, 2020*

Дополнительные источники (ДИ):

№ п/п	Наименование	Автор	Издательство, год издания
[2]	*Организационно-правовое обеспечение информационной безопасности*	*Белов Е.Б., Пржегорлинский В.Н.*	*Академия, 2020*

Интернет-источники:

[3] http://www.fstec.ru - Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

[4] http://www.consultant.ru – Справочно-правовая система «Консультант Плюс»

[5] http://www.garant.ru – Справочно-правовая система «Гарант»

[6] http://www.law.edu.ru – Федеральный правовой портал «Юридическая Россия»

4. Контроль и оценка результатов освоения учебной дисциплины.

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Результаты обучений (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
уметь:	
-классифицировать защищаемую информацию по видам тайны и степеням секретности;	Текущий контроль в форме: выполнение лабораторных работ; устного опроса; тестирований.
- классифицировать основные угрозы безопасности информации.	
знать:	
-сущность и понятие информационной безопасности, характеристику ее составляющих;	Текущий контроль в форме: выполнение лабораторных работ; устного опроса; тестирований.
-место информационной безопасности в системе национальной безопасности страны;	
-виды, источники и носители защищаемой информации;	
-источники угроз безопасности информации и меры по их предотвращению;	
-факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;	
-жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;	
-современные средства и способы обеспечения информационной безопасности;	
-основные методики анализа угроз и рисков информационной безопасности.	