Министерство образования Московской области
Государственное бюджетное профессиональное образовательное учреждение Московской области
«Дмитровский техникум»

ОДОБРЕНО
на заседании ПЦК
«28» августа 2020г.
Протокол № 6

УТВЕРЖДАЮ
Зам. директора по учебно-методической работе
ГБПОУ МО «Дмитровский техникум»
/Н.Е.Горюшкина /
«28» 08 2020г.

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.06. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность: 10.02.01 Организация и технология защиты информации

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Московской области «Дмитровский техникум»

Александровская И.Л.
2021.04.30 10:04:
15+03'00'

Дмитров, 2020г.

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Московской области «Дмитровский техникум»

Разработчик:

1. ПАСПОРТ РАБОЧЕЙ УЧЕБНОЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Область применения рабочей учебной программы

Учебная программа дисциплины является частью образовательной программы в соответствии с ФГОС по специальности **10.02.01 Организация и технология защиты информации**

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена:

П. Профессиональный цикл

ОП. Общепрофессиональные дисциплины

ОП.06. **Основы информационной безопасности**

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

В результате освоения дисциплины студент должен **уметь**:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации.

В результате освоения дисциплины студент должен **знать:**

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности.

Формируемые компетенции:

Общие компетенции

ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы
	выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно–коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Профессиональные компетенции

Код	Наименование видов профессиональной деятельности и профессиональных компетенций
ПК 1.6.	Обеспечивать технику безопасности при проведении организационно-технических мероприятий.
ПК 3.1	Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.
ПК 3.2	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.
ПК 3.3	Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4	Выявлять и анализировать возможные угрозы информационной безопасности объектов.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 72 часов, в том числе: обязательной аудиторной учебной нагрузки обучающегося 48 часов; самостоятельной работы обучающегося 24 часов.

2.СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1.Виды учебной работы и объём учебных часов

Вид учебной работы	**Объём, ч**
Максимальная учебная нагрузка	80
Обязательная аудиторная учебная нагрузка, в том числе	52
практические и семинарские занятия	28
контрольная работа	-
Самостоятельная работа обучающегося	24
Промежуточная аттестация в форме дифференцированного зачёта	

2.2. Тематический план и содержание учебной дисциплины ОП.1 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) *(если предусмотрены)*	Объем часов	Уровень освоения
1	**2**	**3**	**4**
Раздел 1	**Введение**		
Тема 1.1. Информация. Информационные системы: - основные понятия в области обеспечения информационной безопасности - Уровни информационного взаимодействия стр. 12-22			
	Лекции	**2**	
	Семинар	**2**	
	Контрольные работы	**-**	
	Самостоятельная работа студента	**1**	
Раздел 2.	**Информационная безопасность**		
Тема 2.1. Современная ситуация в области информационной безопасности			
	Лекции	**2**	
	Семинар	**2**	
	Контрольные работы		

-защита информации как деятельность -виды и цели защиты информации	Самостоятельная работа студента	**1**	
Тема 2.2. Основные виды и источники атак на информацию			
	Лекции	**4**	
-Естественные угрозы -Искусственные угрозы Источники атак на информацию	Семинар	**2**	
	Контрольные работы		
	Самостоятельная работа студента	**1**	
Тема 2.3. Угроза безопасности информации -внутренние угрозы -внешние угрозы			
	Лекции	**2**	
	Семинар	**2**	
	Контрольные работы		
	Самостоятельная работа студента	**1**	
Тема 2.4. Факторы угроз безопасности информации -понятие «объект защиты информации»			
	Лекции	**2**	
	Семинар	**2**	
	Контрольные работы		
	Самостоятельная работа студента	**1**	

Тема 2.5. Критерии и нормы безопасности информации --виды и цели защиты информации стр.114-119-136			
	Лекции	**2**	
	Семинар	**2**	
	Контрольные работы		
	Самостоятельная работа студента	**1**	
Тема 2.6. Носитель информации как объект защиты -Сущность и определение понятия «Носитель информации» -Документированная информация и информационные ресурсы			
	Комбинированный урок	**2**	
	Семинар	**2**	
	Контрольные работы		
	Самостоятельная работа студента	**1**	
Тема 2.7. Объект информатизации как объект защиты информации -Определение понятия «Объект информатизации»			
	Лекции	**2**	
	Семинар	**2**	
	Контрольные работы		
	Самостоятельная работа студента	**1**	

Компоненты и классификация объектов информатизации			
Раздел 3.	**Современные средства и способы обеспечения информационной безопасности**		
Тема 3.1. Абстрактные модели защиты информации -виды умышленных угроз информации. -модели основных типов политики безопасности			1,3
	Лекции	2	
	Лабораторные работы	2	
	Контрольные работы		
	Самостоятельная работа студента	1	
Тема 3.2. Наиболее распространенные методы взлома -обзор наиболее распространенных методов "взлома"			*1*
	Лекции	4	

	Контрольные работы		
	Самостоятельная работа студента		
Тема 3.3. Средства и способы обеспечения информационной безопасности			*1,2,3*
	Лекции	2	
	Лабораторные работы	2	
	Контрольные работы		

- угрозы обеспечения корпоративной информационной безопасности	Самостоятельная работа студента	1
Тема 3.7. Методы антивирусной защиты информации -антивирусная защита КИС(стр.107-109(2))		
	Лекции	4
	Лабораторные работы	2
	Контрольные работы	
	Самостоятельная работа студента	1
Раздел 4.	**Защита информации в информационных системах**	
Тема 4.1. Общие вопросы комплексной системы защиты информации. - виды каналов утечки (стр.116-119 (2)) конфиденциальной информации		
	Лекции	2
	Лабораторные работы	2
	Контрольные работы	
	Самостоятельная работа студента	2
Тема 4.2. Защита локальных сетей и операционных систем - основные цели сетевой безопасности - методы защиты(лекция из инета)		
	Лекции	4
	Лабораторные работы	2
	Контрольные работы	

	Самостоятельная работа студента	

Тема 4.3. Проблемы защиты информации в Интернет. -Рекомендации по защите информации в Интернет	Лекции	2	
	Лабораторные работы	-	
	Контрольные работы		
	Самостоятельная работа студента	1	
Тема 4.4. Информационная безопасность в Intranet - защита от внешних угроз -комплексное применение криптографических алгоритмов			
	Лекции	4	
	Лабораторные работы	1	
	Контрольные работы		
	Самостоятельная работа студента	2	
Раздел 5	**Автоматизированная система как комплексный объект защиты информации**		
Тема 5.1 Определение понятия «Автоматизированная система» -компоненты АС -классификация			
	Лекции	2	
	Лабораторные работы	-	
	Контрольные работы		
	Самостоятельная работа студента	2	
Тема 5.2. Классификация автоматизированных систем **-АСУ** **-САПР** **-АСОИ**			
	Лекции	4	
	Лабораторные работы	2	
	Контрольные работы		
	Самостоятельная работа студента	1	

Тема 5.3. Информационная война и перспективы развития систем ИБ			
	Лекции	4	
	Лабораторные работы	2	
	Контрольные работы		
	Самостоятельная работа студента	1	
Самостоятельная работа обучающихся		24	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация дисциплины проводится в учебной лекционной аудитории; в компьютерных кабинетах, лабораториях.

Оборудование лабораторий и рабочих мест лабораторий: рабочие места, проектор, ПК, учебное ППО. Состав программного обеспечения: операционная система с графической операционной оболочкой (Microsoft Windows, GNU/Linux), интегрированный пакет прикладных программ офисного назначения и другие. Дополнительно: в составе программного обеспечения файлового менеджера, архиватора, программы просмотра графических изображений с конвертором форматов, растрового и векторного графических Специальные помещения должны представлять собой учебные аудитории для проведения учебных занятий всех типов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенными оборудованием, техническими средствами обучения и материалами, учитывающими требования ФГОС.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» обеспечением доступа в электронную информационно - образовательную среду образовательной организации (при наличии). В случае применения электронного обучения, дистанционных образовательных технологий допускается замена специально оборудованных помещений их виртуальными аналогами, позволяющими обучающимся осваивать УК и ПК.

Образовательная организация должна быть обеспечена необходимым комплектом лицензионного программного обеспечения, состав которого определяется в рабочих программах учебных предметов, курсов, дисциплин (модулей) и подлежит ежегодному обновлению.

3.2. Информационное обеспечение обучения

*Основная литература**

1 Информационная безопасность: учеб./под ред. В.П.,Мельников.- М.: Куприянов А.И 2018. –Рек. ФИРО

Дополнительная литература

2. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография, Смирнов А.А., ЮНИТИ-ДАНА; Закон и право, Москва, 2019

3. Защита информации в компьютерных системах и сетях, Шаньгин В.Ф., ДМК Пресс, Москва, 2017

Методы и средства инженерно-технической защиты информации: учебное пособие, Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р., ФЛИНТА, Москва, 2018

Интернет- ресурсы

1 Exponenta.ru Компания «AXOFT»

2 Vikipedia.org Компания «Vikipedia Foundation»

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения **(освоенные умения, усвоенные знания)**	**Формы и методы контроля и оценки результатов обучения**
Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	Промежуточная аттестация: практическое задание; Текущий контроль: контрольная работа, лабораторная работа
Уметь применять основные правила и документы системы сертификации Российской Федерации	Промежуточная аттестация: практическое задание; Текущий контроль: контрольная работа, лабораторная работа

Уметь классифицировать основные угрозы безопасности информации	Промежуточная аттестация: практическое задание; Текущий контроль: контрольная работа, лабораторная работа
Знать сущность и понятие информационной безопасности, характеристику ее составляющих	Промежуточная аттестация: практическое задание; Текущий контроль: контрольная работа, лабораторная работа
Знать место информационной безопасности в системе национальной безопасности страны	Промежуточная аттестация: практическое задание; Текущий контроль: контрольная работа, лабораторная работа
Знать источники угроз информационной безопасности и меры по их предотвращению	Промежуточная аттестация: практическое задание; Текущий контроль: контрольная работа, лабораторная работа
Знать жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	Промежуточная аттестация: практическое задание; Текущий контроль: контрольная работа, лабораторная работа
Знать современные средства и способы обеспечения информационной безопасности	Текущий контроль: тестирование, контрольная работа

Лист регистрации изменений

Номер изменения	Номер листов	Основание для внесения изменений			Подпись	Расшифровка подписи	Дата	Дата введения изменения
	замененных	новых	Аннулированных					
