ГБПОУ «СТАПМ им.Д.И. Козлова»

УТВЕРЖДАЮ
Зам. директора ГБПОУ
« СТАПМ им.Д.И. Козлова»
_____ Н.В. Кривчун
«17» ____04_____ 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.В.15 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Профессиональный учебный цикл
Общепрофессиональные дисциплины
программы подготовки специалистов среднего звена
09.02.04 Информационные системы (в машиностроении)

2020

ОДОБРЕНО
Цикловой комиссией
общепрофессиональных дисциплин
Председатель _____ Г.В. Муракова
«17» 04 2020 г.

Составитель: Ляпнев А.В. преподаватель ГБПОУ «СТАПМ им. Д.И. Козлова» .

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.04 Информационные системы (по отраслям)(утв. приказом Министерства образования и науки РФ от 14 мая 2014 г. N 525).

Рабочая программа разработана в соответствии с разъяснениями по формированию примерных программ учебных дисциплин начального профессионального и среднего профессионального образования на основе Федеральных государственных образовательных стандартов начального профессионального и среднего профессионального образования, утвержденными И.М. Реморенко, директором Департамента государственной политики и нормативно-правового регулирования в сфере образования Министерства образования и науки Российской Федерации от 27 августа 2009 года.

Содержание программы реализуется в процессе освоения студентами программы подготовки специалистов среднего звена по специальности 09.02.04 Информационные системы (по отраслям) в соответствии с требованиями ФГОС СПО.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.В. 15 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

1.1. Область применения программы

Рабочая программа учебной дисциплины - является частью программы подготовки специалистов среднего звена по специальности 09.02.04 Информационные системы (по отраслям), разработанной в соответствии с ФГОС СПО .

1.2. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина входит в профессиональный цикл как общепрофессиональная дисциплина, вариативная часть.

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

В результате освоения учебной дисциплины обучающийся 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 учебной дисциплины обучающийся 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.

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

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 в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за 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.

ПК 1.1. Собирать данные для анализа использования и функционирования

информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы.

ПК 1.2. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

ПК 1.3. Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения.

ПК 1.4. Участвовать в экспериментальном тестировании информационной системы на этапе опытной эксплуатации, фиксировать выявленные ошибки кодирования в разрабатываемых модулях информационной системы.

ПК 1.7. Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.

ПК 1.9. Выполнять регламенты по обновлению, техническому сопровождению и восстановлению данных информационной системы, работать с технической документацией.

ПК 1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

ПК 2.5. Оформлять программную документацию в соответствии с принятыми стандартами.

ПК 2.6. Использовать критерии оценки качества и надежности функционирования информационной системы.

1.4. Количество часов на освоение программы учебной дисциплины

Максимальная учебная нагрузка обучающегося 153 часа, в том числе:

обязательная аудиторная учебная нагрузка обучающегося 102 часа;

самостоятельная работа обучающегося 51час.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	153
Обязательная аудиторная учебная нагрузка (всего),	102
в том числе:	
практические занятия	40
Самостоятельная работа обучающегося (всего),	51
в том числе: Ответы на контрольные вопросы, подготовка к практическим занятиям, Подготовка сообщений, докладов.	
Промежуточная аттестация в форме дифференцированного зачета	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) (если предусмотрены)	Объем часов	Уровень освоения
1	2	3	4
Основы информационной безопасности			
Раздел 1. Информационная безопасность и уровни ее обеспечения	**Содержание**	**32**	
Тема 1.1. Понятие "информационная безопасность"	Введение.	4	2
	Проблема информационной безопасности общества		
	Самостоятельная работа №1 Подготовка доклада по теме : Значение информационной безопасности для общества. Выдающиеся личности в истории вычислительной техники; Общество в период развития информатизации;	2	
Тема 1.2. Составляющие информационной безопасности	Доступность информации. Целостность информации	14	3
	Конфиденциальность информации		
	Уровни информационной безопасности объектов		
	Обнаружение и противодействие атакам.		
	Криптографические механизмы конфиденциальности, целостности и аутентичности информации		
	Основные возможности криптографических методов защиты информации		
	Человеческий фактор в безопасности.		
	Самостоятельная работа №2 Подготовка ответов на контрольные вопросы: 1. Что такое доступность информации? 2. Что такое конфиденциальная информация,	4	

		государственная и коммерческая тайна? 3. Какие три возможные степени секретности вы знаете? 4. Каковы три категории ценности коммерческой информации? Подготовка доклада по теме: Основные методы определения объема информации.		
Тема 1.3. Система формирования режима информационной безопасности		Задачи информационной безопасности общества	2	2
		Практическая работа №1 Параметры безопасности программы Microsoft Outlook	2	
		Самостоятельная работа №3 Подготовка докладов по темам: Методы создания безопасных систем обработки информации. Угрозы безопасности компьютерных систем.	6	
Тема 1.4. Нормативно-правовые основы информационной безопасности в РФ		Правовые основы информационной безопасности общества	8	3
		Государственная система обеспечения информационной безопасности.		
		Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации		
		Ответственность за нарушения в сфере информационной безопасности		
		Практическая работа № 2 Права на использование директории для определенного пользователя	2	
		Самостоятельная работа№4 Подготовка ответов на контрольные вопросы: 1. Что такое доктрина ИБ РФ? 2. Перечислите основные функции системы обеспечения ИБ РФ 3. Перечислите внешние источники угроз ИБ РФ 4. Назовите внутренние источники угроз ИБ РФ. Подготовка доклада по теме : Общие методы обеспечения ИБ РФ. Правовые основы защиты информации	8	
Раздел 2. Стандарты ИБ		**Содержание**	**36**	
Тема 2.1. Стандарты		Требования безопасности к информационным системам	4	2

информационной безопасности: "Общие критерии"		Принцип иерархии: класс – семейство – компонент – элемент		
		Практическая работа №3 Проверка компьютера на предмет наличия уязвимостей	8	
		Практическая работа №4 Исследование угроз доступности		
		Практическая Работа №5 Использование средств администрирования Windows для анализа и настройки безопасности системы		
		Практическая работа № 6 Использование шифрующей файловой системы		
		Самостоятельная работа №5 Подготовка докладов по темам: Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем.	7	
Тема 2.2. Стандарты информационной безопасности распределенных систем		Сервисы безопасности в вычислительных сетях	4	2
		Администрирование средств безопасности		
		Самостоятельная работа №6 Подготовка доклада по теме: Роль стандартов информационной безопасности	4	
Тема 2.3. Стандарты информационной безопасности в РФ		Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ	4	3
		Документы по оценке защищенности автоматизированных систем в РФ		
		Самостоятельная работа №7 Подготовка доклада по теме: Единые критерии безопасности информационных систем	5	
Тема 2.4. Административный уровень обеспечения информационной безопасности		Цели, задачи и содержание административного уровня	6	2
		Политика безопасности и меры противодействия.		
		Разработка политики информационной безопасности		
Тема 2.5. Классификация угроз "информационной безопасности		Классы угроз информационной безопасности	4	3
		Каналы несанкционированного доступа к информации		
		Практическая работа №7 Разграничение доступа к системам	6	
		Практическая работа №8 Аварийное восстановление		
		Практическая система №9 Защита и восстановление данных на компьютере, используя систему архивации		

		Самостоятельная работа №8 Подготовка доклада по теме. Подготовка отчетов по практическим работам	4	
Раздел 3. Компьютерные вирусы и защита от них		**Содержание**	**32**	
Тема 3.1. Вирусы как угроза информационной безопасности		Компьютерные вирусы и информационная безопасность	6	2
		Воздействия на программно-аппаратные средства защиты информации		
		Характерные черты компьютерных вирусов		
		***Самостоятельная работа :* №9** Подготовка докладов по теме: Виды компьютерных вирусов. Механизмы безопасности используемые для обеспечения конфиденциальности трафика;	5	
Тема 3.2. Классификация компьютерных вирусов		Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям	2	2
Тема 3.3. Характеристика "вирусоподобных" программ		Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. "Intended"-вирусы. Способы заражения программ. Признаки проявления вируса. Методы защиты.	2	3
		Практическая работа №10 Исследование реестра, на предмет возможных уязвимостей для вирусов	22	
		Практическая работа № 11 Приемы работы с защищенными программами		
		Практическая работа № 12 Использование брэндмауэров		
		Практическая работа №13 Использование антивирусных программ		
		Практическая работа № 14 «Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки AVZ.».		
		Практическая работа № 15 Очистка системы		
		Практическая работа № 16 Настройка антивирусной программы, обновление сигнатур.		
		Практическая работа № 17 Оптимизация антивирусной программы под определенную систему		
		Практическая работа № 18 Задание исключений и требований доверия		

		Практическая работа № 19 Борьба с рекламными и шпионскими программами		
		Практическая работа № 20 Настройка межсетевого экрана		
		***Самостоятельная работа :* №10** Подготовка ответов на контрольные вопросы: 1. Каковы основные классификационные признаки компьютерных вирусов? 2. Приведите разновидности файловых вирусов. Подготовка сообщения: -Способы заражения программ. -Методы, средства и технологии борьбы с компьютерными вирусами. В чем особенность компьютерного вируса «Чернобыль»; Хронология развития компьютерных вирусов;	6	
		Диф. зачет	**2**	
		ВСЕГО	**153**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 - ознакомительный (узнавание ранее изученных объектов, свойств)
2 - репродуктивный (выполнение деятельности по образцу, инструкции и под руководством)
3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. УСЛОВИЯ РЕАЛИЗАЦИИ ТИПОВОЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к материально-техническому обеспечению

Реализация программы дисциплины предполагает наличие учебного кабинета.

Оборудование учебного кабинета:

- рабочее место преподавателя;
- рабочие места по количеству обучающихся;
- наглядные пособия (таблицы, схемы и т.д.).

Технические средства обучения:

- компьютер;
- видеопроектор;
- интерактивная доска

3.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, интернет-ресурсов, дополнительной литературы

Основные источники:

1. Клейменов С.А., Мельников В.П. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. Гриф МО РФ. 7-е изд. - М.: Издательство: Академия, 2012. – 336 с.

Дополнительные источники:

2. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие – М.: Финансы и статистика, 2005. – 176 с.

3. С. П. Расторгуев Основы информационной безопасности – М.: Академия, 2007. – 192 с.

4. Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов Основы информационной безопасности – М.: Горячая Линия – Телеком, 2006. – 544 с.

5. 4. Цирлов В.Л. Основы информационной безопасности: краткий курс/Профессиональное образование. – М.: Феникс, 2008. – 400 с.

Интернет-ресурсы:

1. http://fcior.edu.ru/ - Федеральный центр информационно-образовательных ресурсов

2. http://www.edu.ru/ - Федеральные образовательные ресурсы

3. http:// www.adinf.ru – Web-сайт разработчиков антивируса ADinf.

4. http:// www.dials.ru – сервер антивирусной лаборатории.

5. http:// www.symantec.ru – Российское интернет-представительство компании Symantec, производящей антивирусный пакет Norton AntiVirus.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формируемые общие и профессиональные компетенции**	**Формы и методы контроля и оценки результатов обучения**
Умение классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; Умение применять основные правила и документы системы сертификации Российской Федерации; Умение классифицировать основные угрозы безопасности информации. Знание сущности и понятия информационной безопасности, характеристики ее составляющих; Знание места информационной безопасности в системе национальной безопасности страны; Знание источников угроз информационной безопасности и меры по их предотвращению; Знание жизненных циклов конфиденциальной информации в процессе ее создания, обработки, передачи; Знание современных средств и способов обеспечения информационной безопасности.	ОК 1-ОК 9	Оценка результатов деятельности обучающихся при выполнении и защите результатов практических занятий, тестировании, внеаудиторной самостоятельной работы, других видов текущего контроля. Оценка результатов деятельности обучающихся при выполнении и защите результатов практических занятий, тестировании, внеаудиторной самостоятельной работы, и других видов текущего контроля.