ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «САРОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОЦИАЛИСТИЧЕСКОГО ТРУДА БОРИСА ГЛЕБОВИЧА МУЗРУКОВА»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности среднего профессионального образования
10.02.01 Организация и технология защиты информации

2021г.

Рабочая программа учебной дисциплины ОП.06 Основы информационной безопасности разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) для специальности среднего профессионального образования 10.02.01 Организация и технология защиты информации.

Организация – разработчик: ГБПОУ СПТ им. Б.Г. Музрукова

Разработчик: И.В.Столяров, преподаватель ГБПОУ СПТ им. Б.Г. Музрукова

СОГЛАСОВАНО
Протокол № 1 от «30» 08 2021 г.
Председатель МК
_____ Е.Н. Маресева

УТВЕРЖДАЮ
Зам. директора по УР
_____ О.Н. Тарасова
«02» 09 2021 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.06 Основы информационной безопасности

1.1 Область применения программы

Рабочая программа учебной дисциплины ОП.06 Основы информационной безопасности является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.01 Организация и технология защиты информации.

Программа учебной дисциплины может быть использована в дополнительном профессиональном образовании при реализации программ повышения квалификации и профессиональной подготовки по профессии рабочих 16199 Оператор электронно-вычислительных машин.

1.2 Место учебной дисциплины в структуре основной профессиональной образовательной программы: дисциплина входит в общепрофессиональный цикл.

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;

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.

1.4. Рекомендуемое количество часов на освоение рабочей программы учебной дисциплины

Максимальная учебная нагрузка обучающегося 136 часов, в том числе:
обязательная аудиторная учебная нагрузка обучающегося 94 часа;
самостоятельная работа обучающегося 42 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**136**
Обязательная аудиторная учебная нагрузка (всего),	**94**
в том числе:	
практические занятия	**28**
Самостоятельная работа обучающегося (всего),	**42**
в том числе:	
Итоговая аттестация в форме **экзамена**	

2.2. Тематический план и содержание учебной дисциплины ОП.06 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся,		Объем часов	Уровень освоения
1	2		3	4
Раздел 1. Информационная безопасность и уровни ее обеспечения			**28**	
Тема 1.1. Понятие "информационная безопасность"	**Содержание.**		**6**	
	1	Введение.		1
	2	Проблема информационной безопасности общества.		2
	3	Основные положения государственной политики РФ в информационной сфере.		2
Тема 1.2. Составляющие информационной безопасности	**Содержание.**		**4**	
	1	Доступность информации. Целостность информации.		3
	2	Конфиденциальность информации.		2
Тема 1.3. Система формирования режима информационной безопасности	**Содержание.**		**6**	
	1	Задачи информационной безопасности общества		2
	2	Комплексное обеспечение информационной безопасности РФ		2
	Практическая работа		**2**	3
	1	Параметры безопасности программы Microsoft Outlook		
Тема 1.4. Нормативно-правовые основы информационной безопасности в РФ	**Содержание.**		**12**	
	1	Правовые основы информационной безопасности общества		2
	2	Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации		2
	3	Ответственность за нарушения в сфере информационной безопасности		2
	4	Международные нормативно-правовые акты обеспечения ИБ.		2
	5	Категории объектов и защита ИС.		2
	Практическая работа		**2**	3
	1	Права на использование директории для определенного пользователя		
Раздел 2. Стандарты ИБ			**38**	
Тема 2.1. Стандарты информационной безопасности: "Общие критерии"	**Содержание.**		**14**	
	1	Требования безопасности к информационным системам		1,2
	2	Принцип иерархии: класс – семейство – компонент – элемент		2
	3	Критерии и классы оценки защищённости объектов и деятельности.		2

	Практические работы		**8**	
	1	Проверка компьютера на предмет наличия уязвимостей		3
	2	Исследование угроз доступности		
	3	Использование средств администрирования Windows для анализа и настройки безопасности системы		
	4	Использование шифрующей файловой системы		
Тема 2.2. Стандарты информационной безопасности распределенных систем	**Содержание.**		**6**	
	1	Сервисы безопасности в вычислительных сетях		2,3
	2	Администрирование средств безопасности		2
	3	Программно-аппаратные средства обеспечения ИБ в вычислительных сетях.		2
Тема 2.3. Стандарты информационной безопасности в РФ	**Содержание.**		**6**	
	1	Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ		2
	2	Документы по оценке защищенности автоматизированных систем в РФ		2
	3	Документы, регламентирующие деятельность в области защиты информации.		2
Тема 2.4. Административный уровень обеспечения информационной безопасности	**Содержание.**		**4**	
	1	Цели, задачи и содержание административного уровня		2
	2	Разработка политики информационной безопасности		2
Тема 2.5. Классификация угроз "информационной безопасности	**Содержание.**		**8**	
	1	Классы угроз информационной безопасности		2,3
	2	Каналы несанкционированного доступа к информации		2
	Практические работы		**4**	
	1	Аварийное восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.		3
	2	Защита и восстановление данных на компьютере, используя систему архивации		
Раздел 3. Компьютерные вирусы и защита от них			**28**	
Тема 3.1. Вирусы как угроза информационной безопасности	**Содержание.**		**4**	
	1	Компьютерные вирусы и информационная безопасность		2
	2	Характерные черты компьютерных вирусов		2
Тема 3.2. Классификация компьютерных вирусов	**Содержание.**		**2**	
	1	Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям		2
Тема 3.3. Характеристика "вирусоподобных" программ	**Содержание.**		**22**	
	1	Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. "Intended"-вирусы		1
	2	Оптимизация антивирусной программы под определенную систему		2

	3	Задание исключений и требований доверия		2
	4	Борьба с рекламными и шпионскими программами		2
	5	Настройка межсетевого экрана		2
	Практические работы		**12**	
	1	Исследование реестра, на предмет возможных уязвимостей для вирусов		2,3
	2	Использование брандмауэра для анализа трафика между двумя сетями.		
	3	Использование антивирусных программ для защиты компьютера.		
	4	Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки AVZ на ОС WINDOWS.		
	5	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.		
	6	Настройка антивирусной программы, обновление сигнатур.		
Самостоятельная работа при изучении дисциплины Основы информационной безопасности Выдающиеся личности в истории вычислительной техники. Общество в период развития информатизации. Понятие государственной тайны. Отличия функциональных требований от требований доверия Механизмы безопасности используемые для обеспечения конфиденциальности трафика. Категории государственных информационных ресурсов. Ответственность за использование и распространение вредоносных программ для ЭВМ. Механизм обеспечения ИБ в вычислительных сетях. Особенность компьютерного вируса «Чернобыль». Хронология развития компьютерных вирусов. История криптографической деятельности. Простейшие шифры и их свойства. Ключевые системы разграничения доступа и электронная цифровая связь. Методы и средства ограничения доступа к компонентам ЭВМ. Системы опознавания нарушителей. Автоматизация технического контроля защиты потоков информации. Защита процессов переработки информации в СУБД. Отечественное нормативно-правовое обеспечение ИБ. Технологии предотвращения угроз ИБ. Модели защиты при отказе в обслуживании. Области и сферы обеспечения ИБ.			**42**	
Всего:			**94**	
Итого:			**136**	

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 УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к материально-техническому обеспечению

Реализация программы дисциплины предполагает наличие учебного кабинета общепрофессиональных дисциплин и профессиональных модулей по направлению Информационная безопасность, лаборатории программно-аппаратных и технических средств защиты информации, электронного документооборота.

Оборудование учебного кабинета:

- рабочее место преподавателя;
- комплект учебно-методической документации;
- 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:

Нестеров С.П. Информационная безопасность: Учебник и практикум для СПО. – М.: Юрвайт, 2019.

Рекомендуемые источники:

1. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие – М.: Финансы и статистика, 2005. – 176 с.
2. С. П. Расторгуев Основы информационной безопасности – М.: Академия, 2007. – 192 с.
3. Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов Основы информационной безопасности – М.: Горячая Линия – Телеком, 2006. – 544 с.
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 работ, тестирования, а также выполнения обучающимися индивидуальных заданий, исследований.

Результаты обучения (освоенные умения, освоенные знания)	**Формы методы контроля и оценки результатов обучения**
Умения;	
классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	Устный опрос
применять основные правила и документы системы сертификации Российской Федерации	Практические занятия
классифицировать основные угрозы безопасности информации	Практические занятия
Знания;	
сущности и понятия информационной безопасности, характеристики ее составляющих	Устный опрос
места информационной безопасности в системе национальной безопасности страны	Тестирование
источников угроз информационной безопасности и меры по их предотвращению	Практические занятия
жизненных циклов конфиденциальной информации в процессе ее создания, обработки, передачи	Устный опрос
современных средств и способов обеспечения информационной безопасности	Практические занятия