Министерство образования и молодежной политики Свердловской области
государственное автономное профессиональное образовательное учреждение
Свердловской области
«Уральский радиотехнический колледж им. А.С. Попова»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 «Основы информационной безопасности»

для специальности среднего профессионального образования

10.02.03 Информационная безопасность автоматизированных систем

базового уровня подготовки

2020 г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта специальности среднего профессионального образования 10.02.03 Информационная безопасность автоматизированных систем

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Д.В. Колесников
«_30__» ____06_____ 2020 г.

Рекомендована цикловой методической комиссией
«Электронных вычислительных машин»
Протокол от «__29__»___06_____ 2020 г. №__6__
Председатель ЦМК _____Ю. Г.К отова

Разработчик:

Поликарпова С.В., преподаватель

Рецензенты:

Уймин А. Г., преподаватель УРТК им. А. С. Попова

СОДЕРЖАНИЕ

1 ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 6

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 12

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ 14

1 ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01 Основы информационной безопасности

1.1 Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 10.02.03 Информационная безопасность автоматизированных систем, базового уровня подготовки

1.2 Место дисциплины в структуре основной профессиональной образовательной программы: общепрофессиональная дисциплина профессионального цикла

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

В результате освоения 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 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;

Дисциплина способствует формированию следующих общих компетенций (ОК) и профессиональных компетенций (ПК):

– 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 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 2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.

– ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.

– ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.

– ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

1.4 Количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 110 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 74 часа;
самостоятельной работы обучающегося 36 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**110**
Обязательная аудиторная учебная нагрузка (всего)	**74**
в том числе:	
лабораторные занятия	**0**
практические занятия	**24**
Самостоятельная работа обучающегося (всего)	**36**
в том числе:	
Изучение литературы Оформление отчета	**36**
Итоговая аттестация в форме экзамена	

2.2 Тематический план и содержание учебной дисциплины ОП.03 «Архитектура аппаратных средств»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Тема 1 Политика и концепции информационной безопасности	**Содержание учебного материала**	14	
	1. Понятие информации. Информация как объект защиты.		2
	2. Понятие информационной безопасности. Основные составляющие.		2
	3. Понятие и концепции информационной войны		2
	4. Понятие и концепции информационной войны		2
	5. Политика информационной безопасности		2
	6. Концепции информационной безопасности		2
	7. Концепции информационной безопасности		2
	Самостоятельная работа обучающихся Изучение литературы, подготовка к тесту	8	
Тема 2 Уязвимость информации	**Содержание учебного материала**	6	2
	1. Защищаемая информация. Степени конфиденциальности.		2
	2. Виды уязвимости информации и формы ее проявления.		2
	3. Виды уязвимости информации и формы ее проявления		2
	Самостоятельная работа обучающихся Изучение литературы, подготовка к тесту	4	
Тема 3 Защита информации в автоматизированных системах	**Содержание учебного материала**	28	2
	1. Классификация атак на информационные системы		
	2. Классификация атак на информационные системы		2
	3. Источники угроз информационной безопасности и меры по их предотвращению		2
	4. Каналы и методы НСД к защищаемой информации		2
	5. Носители защищаемой информации. Объекты. Виды		2
	6. Система сертификации средств защиты информации		2
	7. Центр безопасности Windows		2
	8. Методологические подходы к защите информации и принципы ее организации		2
	9. Защита информации средствами разграничения прав доступа		2
	10. Криптографические методы защиты информации		2
	11. Шифрование файлов и дисков		2
	12. Реестр Windows		
	Практические работы	24	
	1. Практическая работа №1 «Разграничения прав доступа»		
	2. Практическая работа №1 «Разграничения прав доступа»		
	3. Практическая работа №2 «Центр безопасности Windows»		
	4. Практическая работа №2 «Центр безопасности Windows»		
	5. Практическая работа №3 «Локальные политики безопасности»		
	6. Практическая работа №3 «Локальные политики безопасности»		
	7. Практическая работа №4. «Шифрование файлов EFS»		
	8. Практическая работа №4 «Шифрование файлов EFS»		

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
	9. Практическая работа №5 «Шифрование дисков»		
	10. Практическая работа №5 «Шифрование дисков»		
	11. Практическая работа №6 «Реестр Windows»		
	12. Практическая работа №6 «Реестр Windows»		
	Самостоятельная работа обучающихся Изучение литературы, конспекта. Оформление отчетов, подготовка к защите практических работ.	24	
	Дифференцированный зачет	2	
	Всего:	**110**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы дисциплины требует наличия лаборатории аппаратных средств вычислительной техники, инженерно-технической средств обеспечения информационной безопасности и мастерской «Кибербезопасность».

Технические средства обучения: проектор, персональный компьютер.

Оборудование лаборатории и рабочих мест лаборатории:

– Персональный компьютер

– Проектор

Программное обеспечение:

– Операционная система Windows xx;

– Оборудование мастерской «Кибербезопасность»:

– ПЭВМ в сборе (i7/32Gb MEM/ 256Gb + 1Tb nvme SSD/ Nvidia Qadro 1000 / Intel 4x1Gb/s Lan Card/ 27” Monitor)

– Epson EB-2247U

– Экран для проектора Lumien Master Picture 191x300 Matte White FiberGlass

– Рабочее место в сборе:

- стол (ШхД) 1200x750;
- рама задняя длинная;
- перфопанель – 4;
- набор держателей;
- электроблок на 8 розеток;
- полка приборная длинная;
- светильник светодиодный – 2 шт;
- кронштейн для монитора;
- полка для системного блока;
- стул тканевый с металлической крестовиной;
- металлические колеса для стула;
- набор подлокотников.

– Стол для преподавателя

– Стулья для брифинг зоны

– Стол для брифинг зоны (переговорный)

– Вешалка

– Корзина для мусора

– Корзина для бахил

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1) Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана.

2) Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] : справочное пособие / Г.А. Бузов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2018. — 586 с. — Режим доступа: https://e.lanbook.com/book/111027. — Загл. с экрана.

3) Программно-аппаратные средства защиты информации [Электронный ресурс] : учебное пособие / Л.Х. Мифтахова [и др.]. — Электрон. дан. — Санкт-Петербург : ИЦ Интермедия, 2018. — 408 с. — Режим доступа: https://e.lanbook.com/book/103200. — Загл. с экрана.

Дополнительные источники:

1) Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2017.

2) Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации [Электронный ресурс] / А.С. Масалков. — Электрон. дан. — Москва : ДМК Пресс, 2018. — 226 с. — Режим доступа: https://e.lanbook.com/book/105842. — Загл. с экрана.

3) Стеганографические и криптографические методы защиты информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: https://e.lanbook.com/book/90963. — Загл. с экрана.

4) Информационный мир XXI века. Криптография – основа информационной безопасности [Электронный ресурс] / под ред. Э.А. Болелова. — Электрон. дан. — Москва : Дашков и К, 2018. — 126 с. — Режим доступа: https://e.lanbook.com/book/103793. — Загл. с экрана.

5) Информационная безопасность Т. Л Партыка, И. И. Попов М: ФОРУМ: ИНФРА _ М, 2012

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, проведения и защиты лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий (решение задач). Промежуточная аттестация в форме дифференцированного зачета проводится в форме собеседования, обучающие отвечают устно на один теоретический вопрос, и письменно выполняют практическое задание. Итоговая аттестация по дисциплине в

форме экзамена проводится в форме собеседования. Обучающиеся устно отвечают на два теоретических вопроса и письменно выполняют практическое задание билета.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Освоенные умения: - классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - применять основные правила и документы системы сертификации Российской Федерации; -классифицировать основные угрозы безопасности информации;	Устные вопросы по прошедшим лекциям. Проведение тестирования по данным темам. Защита практических работ по темам 1-24.
Усвоенные знания: - 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	Устные вопросы по прошедшим лекциям. Проведение тестирования по данным темам. Дифференцированный зачет.