УТВЕРЖДАЮ
Директор ЧПОУ «КУП»

Документ подписан электронной подписью
Сертификат: 01D70ABAF73B435000000000D29530002
Владелец: Батрак Андрей Анатольевич
Действителен: с 24.02.2021 по 24.02.2022

А.А.Батрак
« 01 » апреля 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.15 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность СПО: 09.02.07 Информационные системы и программирование

на базе среднего общего образования, на базе основного общего образования

Форма обучения **очная**
(очная, заочная, очно-заочная)

Срок освоения **2года 10 месяцев, 3 года 10 месяцев**

Москва
2021

Рабочая программа разработана с учетом требований ФГОС СОО, ФГОС СПО 09.02.07 Информационные системы и программирование и профиля профессионального образования

Организация разработчик: Частное профессиональное образовательное учреждение «Колледж управления и производства»

Заместитель директора по МР

_____С.Х. Морозова

30.03.2021

СОДЕРЖАНИЕ

стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.15 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной образовательной программы в соответствии с ФГОС СПО 09.02.07 Информационные системы и программирование

1.2. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина входит в профессиональный цикл как общепрофессиональная дисциплина. Дисциплина относится к вариативной части профессионального цикла структуры ППССЗ по специальности 09.02.07 Информационные системы и программирование

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

–

Код ПК, ОК	Умения	Знания
ОК 1 – ОК 11	У1 Использовать современные программно-аппаратные средства защиты информации У2 Подобрать и обеспечить защиту информации	З1 Современные законы, стандарты, методы и технологии в области защиты информации З2 Требования к защите информации определенного типа

При угрозе возникновения и (или) возникновении отдельных чрезвычайных ситуаций, введении режима повышенной готовности или чрезвычайной ситуации на всей территории Российской Федерации либо на ее части реализация рабочей программы учебной дисциплины может осуществляться с применением электронного обучения, дистанционных образовательных технологий**.**

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем образовательной программы и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы	**54**
в том числе:	
теоретическое обучение	33
практические занятия	18
Самостоятельная работа	3

Промежуточная(итоговая) аттестация в форме дифференцированного зачета	-

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов	Коды компетенции, формированию которых способствует элемент программы
1	2		3	4
	6 (4)семестр		**51**	
Раздел 1. Информационная безопасность и уровни ее обеспечения				
Тема 1.1. Понятие "информационная безопасность"	**Содержание материала**	**Уровень освоения**	2	ОК1-11
	1 Введение	2		
	2 Проблема информационной безопасности общества	2		
	Самостоятельная работа *Доклад на тему:* Источники и содержание угроз в информационной сфере.		-	
Тема 1.2. Составляющие информационной безопасности	**Содержание материала**	**Уровень освоения**	2	ОК1-11
	1 Доступность информации. Целостность информации	2		
	2 Конфиденциальность информации	2		
	Самостоятельная работа*:* изучить основные показатели конфиденциальности		-	
Тема 1.3. Система формирования режима информационной безопасности	**Содержание материала**	**Уровень освоения**	2	ОК1-11
	1 Задачи информационной безопасности общества	2		
	Практическая работа		2	
	Изучение характеристик составляющих информационной безопасности.			
	Самостоятельная работа: источники и содержание угроз в информационной сфере.		-	
Тема 1.4. Нормативно-	**Содержание материала**	**Уровень освоения**	2	

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов	Коды компетенции, формированию которых способствует элемент программы
1	2		3	4
правовые основы информационной безопасности в РФ	1 Правовые основы информационной безопасности общества	2		ОК1-11
	2 Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации	2		
	3 Ответственность за нарушения в сфере информационной безопасности	2		
	Практическая работа		2	
	1.Права на использование директории для определенного пользователя			
	Самостоятельная работа - изучить основные положения Доктрины информационной безопасности		-	
Раздел 2. Стандарты ИБ				
Тема 2.1. Стандарты информационной безопасности: "Общие критерии"	**Содержание материала**	**Уровень освоения**		
	1 Международный стандарт информационной безопасности (ISO). Система международных и национальных стандартов безопасности информации.	2	4	ОК1-11
	Практическая работа		2	
	1. Проверка компьютера на предмет наличия уязвимостей			
	2. Исследование угроз доступности			
	3. Использование средств администрирования Windows для анализа и настройки безопасности системы			
	4. Использование шифрующей файловой системы			
	Самостоятельная работа Подготовка Реферата по теме Отечественные стандарты безопасности		-	
Тема 2.2. Стандарты	**Содержание материала**	**Уровень освоения**	2	

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)			Объем часов	Коды компетенции, формированию которых способствует элемент программы
1	2			3	4
информационной безопасности распределенных систем	1	Сервисы безопасности в вычислительных сетях	2		ОК1-11
	2	Стандарты и нормативно-методические документы в области обеспечения информационной безопасности.	2		
	Самостоятельная работа*: отличия функциональных требований от требований доверия*			-	
Тема 2.3. Стандарты информационной безопасности в РФ	**Содержание материала**		**Уровень освоения**	2	
	1	Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ	2		ОК1-11
	2	Документы по оценке защищенности автоматизированных систем в РФ.	2		
	Самостоятельная работа: механизмы безопасности используемые для обеспечения конфиденциальности трафика			-	
Тема 2.4. Административный уровень обеспечения информационной безопасности	**Содержание материала**		**Уровень освоения**	3	
	1	Цели, задачи и содержание административного уровня	2		ОК1-11
	2	Разработка политики информационной безопасности	2		
	Самостоятельная работа: первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.			-	
Тема 2.5. Классификация угроз "информационной безопасности	**Содержание материала**		**Уровень освоения**	2	
	1	Классы угроз информационной безопасности	2		ОК1-11
	2	Каналы несанкционированного доступа к информации	2		
	3	Механические системы защиты.	2		
	4	Системы оповещения о попытках вторжения.	2		
	5	Системы опознавания нарушителей.	2		
	6	Авторизация технического контроля защиты потоков информации	2		

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов	Коды компетенции, формированию которых способствует элемент программы
1	2		3	4
	Практическая работа		2	
	1 Аварийное восстановление			
	2 Защита и восстановление данных на компьютере, используя систему архивации			
	Самостоятельная работа*:* ответственность за использование и распространение вредоносных программ для ЭВМ		-	
Раздел 3. Компьютерные вирусы и защита от них				
Тема 3.1. Вирусы как угроза информационной безопасности	**Содержание материала**	**Уровень освоения**	4	
	1 Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов.	2		ОК1-11
	2 Методы и технологии борьбы с компьютерными вирусами. Антивирусные программы. Классификация антивирусных программ. Антивирусные программы Dr Web, Kaspersky, NOD-32.	2		
	Самостоятельная работа обзор современных антивирусных программ Dr Web, Kaspersky, NOD-32. Подготовка Реферата по теме Антивирусные программы		-	
Тема 3.2. Классификация компьютерных вирусов	**Содержание материала**	**Уровень освоения**		
	1 Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям.	2	4	ОК1-11
	Практическая работа		2	
	1 Исследование реестра, на предмет возможных уязвимостей для вирусов			
	2 Использование брандмауэров			
	3 Использование антивирусных программ			

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов	Коды компетенции, формированию которых способствует элемент программы
1	2		3	4
	4 Защита информации от копирования.			
	5 Защита информации от несанкционированного доступа.			
	Самостоятельная работа Выполнение индивидуального задания		-	
Тема 3.3. Характеристика "вирусоподобных" программ	**Содержание материала**	**Уровень освоения**	4	ОК1-11
	1 Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. "Intended"-вирусы. Защита информации в сетях. Сервисы безопасности. Межсетевые экраны – брандмауэры. Прокси – серверы. Системы активного аудита	2		
	Практическая работа		8	
	1 Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки AVZ.			
	2 Очистка системы			
	3 Настройка антивирусной программы, обновление сигнатур.			
	4 Оптимизация антивирусной программы под определенную систему			
	5 Задание исключений и требований доверия			
	6 Борьба с рекламными и шпионскими программами			
	7 Настройка межсетевого экрана			

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)			Объем часов	Коды компетенции, формированию которых способствует элемент программы
1	**2**			**3**	**4**
	8	**Самостоятельная работа** изучить Технические регламенты защиты информации в сетях.		3	
Промежуточная (итоговая) аттестация	**Дифференцированный зачет**				
			Объем образовательной программы (ВСЕГО):	**54**	

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 РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к материально-техническому обеспечению

Реализация программы дисциплины предполагает наличие учебного кабинета.

Многофункциональный кабинет
Оборудование:
персональные компьютеры (ЖК монитор, системный блок, клавиатура, мышка) имеющие выход в Интернет – 16 шт.; веб-камера -1 шт.; МФУ – 1 шт.; принтер цветной – 1 шт.; комплект стереоколонок – 1 шт.; интерактивная доска – 1 шт.; мультимедийный проектор – 1 шт.; маркерная доска передвижная – 1 шт.; учебная мебель (стол и стул преподавателя, парты – 21 шт., стулья – 27 шт., шкаф – 2 шт.).
Программное обеспечение:
- Microsoft Windows;
- Пакет Microsoft Office;

- Notepad++.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, интернет-ресурсов, дополнительной литературы

Основные источники:

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ИНФОРМАЦИИ 2-е изд., испр. и доп. Учебное пособие для СПО Средства обеспечения безопасности компьютерных сетей http://www.biblio-online.ru/book/B3751835-9BAC-40BE-99EF-B8D50EEA4327

Внуков А. А. Национальный исследовательский университет «Высшая школа экономики» (г. Москва) Профессиональное образование Гриф УМО СПО 2019 240

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Учебник и практикум для СПО http://www.biblio-online.ru/book/585588B5-9A99-461C-A399-E93A7C96120A

Нестеров С. А. Санкт-Петербургский политехнический университет Петра Великого (г. Санкт-Петербург). Профессиональное образование Гриф УМО СПО 2019 321

Дополнительные источники:

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ. Учебное пособие для СПО http://www.biblio-online.ru/book/B1530BFC-7C8E-469A-B783-2F698B029EB8

Казарин О. В., Шубинский И. Б. Московский государственный университет имени М.В. Ломоносова (г. Москва).;Российский государственный гуманитарный университет (г. Москва). Профессиональное образование Гриф УМО СПО 2019

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.

3.3.Используемые технологии обучения

В целях реализации компетентностного подхода в образовательном процессе используются следующие активные и интерактивные формы проведения занятий: анализ конкретных ситуаций, круглый стол (групповые дискуссии и дебаты), мозговой штурм или брейнсторминг, интернет-экскурсии (интерактивная экскурсия), олимпиада, конференция, работа в малых группах, социальные проекты (внеаудиторные формы - соревнования, фильмы, спектакли, выставки и др.), интерактивные лекции (применением видео- и аудиоматериалов) и др.

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, исследований.

Результаты обучения	**Критерии оценки**	**Формы и методы оценки**
Перечень умений, осваиваемых в рамках дисциплины: У1 Использовать современные программно-аппаратные средства защиты информации У2 Подобрать и обеспечить - защиту информации *Перечень знаний, осваиваемых в рамках дисциплины:* З1 Современные законы, стандарты, методы и технологии в области защиты информации З2 Требования к защите информации - определенного типа	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного	•Компьютерное тестирование на знание терминологии по теме; Тестирование…. Контрольная работа Самостоятельная работа. Защита реферата…. Наблюдение за выполнением практического задания. (деятельностью студента) Оценка выполнения практического задания(работы) Подготовка и выступление с докладом, сообщением, презентацией… Решение ситуационной задачи….

	характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	