Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курский государственный университет»

Колледж коммерции, технологий и сервиса

УТВЕРЖДЕНО
протокол заседания
ученого совета от 31.08.2016 г., № 1

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Курск 2016

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО) **09.02.05 Прикладная информатика (по отраслям)** (базовой подготовки).

Организация – разработчик: ФГБОУ ВО «Курский государственный университет».

Разработчик:

Ефимцева И.Б. – преподаватель колледжа коммерции, технологий и сервиса ФГБОУ ВО «Курский государственный университет».

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
Информационная безопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью ППССЗ в соответствии с ФГОС по специальности СПО **09.02.05 Прикладная информатика (по отраслям).**

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки).

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

дисциплина входит в профессиональный цикл

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

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

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-комммуникационные 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
ПК 1.5	Контролировать работу компьютерных, периферийных устройств и телекоммуникационных систем, обеспечивать их правильную эксплуатацию
ПК 3.1	Разрешать проблемы совместимости программного обеспечения отраслевой направленности

ПК 3.3	Проводить обслуживание, тестовые проверки, настройку программного обеспечения отраслевой направленности

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

– определять необходимый уровень безопасности информации;

– распознавать воздействие вируса на программный продукт или данные;

– противодействовать вирусной атаке;

– использовать антивирусные программы;

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

– виды объектов, подлежащих защите, необходимость защиты информации;

– источники и пути реализации несанкционированного доступа к информации;

– уровни информационной безопасности объектов;

– виды и назначение различных мер обеспечения информационной безопасности;

– особенности использования технических и программно-математических мер;

– назначение и место использования идентификации и аутентификации;

– необходимость использования разграничения доступа;

– основные возможности криптографических методов защиты информации;

– пути проникновения компьютерных вирусов;

– классификацию деструктивных воздействий вируса;

– средства защиты от воздействия вирусов;

– виды и назначение антивирусных программ;

– методы профилактики заражения вирусами;

– основные международные правовые акты по защите информации;

– основные положения и принципы международных соглашений;

– соответствие российских и международных правовых соглашений;

– российские общегосударственные правовые документы по защите информации;

– российские отраслевые нормативные документы по защите информации;

– назначение должностных инструкций;

– методы контроля за исполнением должностных инструкций.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 72 часа, в том числе:
обязательной аудиторной учебной нагрузки обучающегося 48 часов;
самостоятельной работы обучающегося 24 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)	72
Обязательная аудиторная учебная нагрузка (всего)	48
в том числе:	
лабораторные занятия	-
практические занятия	10
контрольные работы	-
Самостоятельная работа обучающегося (всего)	24*
Подготовка рефератов, докладов. Изучение материала, вынесенного на самостоятельную проработку. Оформление отчетов по практическим работам	16* 2* 6*
Итоговая аттестация в форме *дифференцированного зачета*	

* в т.ч. 4 часа консультаций

2.2. Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работа (проект) *(если предусмотрены)*		Объем часов	Уровень освоения
1	**2**		**3**	**4**
Раздел 1. Борьба с угрозами несанкционированного доступа к информации			30	
Тема 1.1. Актуальность, проблемы обеспечения безопасности информации	**Содержание**		8	
	1	**Введение в дисциплину** Введение. Учебная дисциплина «Информационная безопасность», ее основные задачи и связь с другими дисциплинами. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации.	6	1
	2	**Основные понятия информационной безопасности** Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации		1
	3	**Угрозы информационной безопасности** Классификация угроз информационной безопасности, источники возникновения и пути реализации. Определение требований к уровню обеспечения информационной безопасности		
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Информационная безопасность деятельности общества и ее основные поло-		2	

	жения			
Тема 1.2. Виды мер обеспечения информационной безопасности	**Содержание**		10	
	1	**Виды мер обеспечения информационной безопасности** Законодательные, морально-этические, организационные, технические, программно-математические меры обеспечения информационной безопасности	6	2
	2	**Специфические приемы управления техническими средствами** Приемы управления техническими средствами		1
	3	**Меры обеспечения информационной безопасности** Методы защиты от копирования. Некопируемые метки. Защита от средств отладки и дисассемблирования. Защита от трассировки по заданному прерыванию. Защита программ в оперативной памяти.		2
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Области и сферы по обеспечению информационной безопасности Стратегии обеспечения информационной безопасности фирм		4[1]	
Тема 1.3. Основные принципы построения систем защиты информации	**Содержание**		12	
	1	**Основные защитные механизмы** Идентификация и аутентификация: понятие, назначение, место использования. Необходимость использования разграничения доступа.	6	
	2	**Основные возможности криптографических методов защиты информации** Контроль целостности. Криптографические механизмы конфиденциальности, целостности и аутентичности информации		
	3	**Обнаружение и противодействие атакам** Системы обнаружения атак на уровне сети. Обнаружение и противодей-		

[1] в т.ч. 1 час консультаций

		ствие информационным атакам из Интернета. Системы обнаружения беспроводных атак, принципов их работы и места в комплексе средств обеспечения безопасности беспроводной сети.		
	Практические занятия		2	
	1	Защита информации в компьютерной системе от случайных угроз		
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Способы шифрования Оформление отчета по практическим работам		4[2]	
Раздел 2. **Борьба с вирусным заражением информации**			34	
Тема 2.1. Проблема вирусного заражения и структура современных вирусов	**Содержание**		22	
	1	**Основные сведения о компьютерных вирусах** Компьютерный вирус: понятие, классификация по среде обитания вируса; по способу заражения среды обитания; по деструктивным возможностям; по особенностям алгоритма вируса. Основные пути возникновения и распространения вирусов. Проявление действия вируса	8	1
	2	**Структура современных вирусов** Модели поведения вирусов. Классификация деструктивных действий вируса. Разрушение программы защиты, схем контроля или изменения состояния программной среды. Воздействия на программно-аппаратные средства защиты информации		2
	3	**Программы-шпионы. Взлом парольной защиты** Программные закладки. Классификация программных закладов по методы их внедрения. Группы деструктивных действий, которые могут осу-		2

[2] в т.ч. 1 час консультаций

		ществляться программными закладками. Перехват. Искажение. Уборка мусора. Наблюдение и компрометация. Защита от программных закладок. Клавиатурные шпионы. Парольная защита операционных систем. Взлом парольной защиты операционной системы Windows.		
	4	**Средства защиты от воздействия вирусов** Защита от воздействия вирусов		3
	Практические занятия		6	
	1	Приемы работы с защищенными программами		
	2	Перехват вывода на экран		
	3	Перехват ввода с клавиатуры		
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Модели защиты при отказе в обслуживании История криптографической деятельности - оформление отчетов по практическим работам		8[3]	
Тема 2.2. Классификация антивирусных программ	**Содержание**		12	
	1	**Программы-детекторы, программы-доктора** Назначение, классификация, недостатки, принцип действия программ-детекторов. Назначение, принцип действия программ-доктора.	6	1
	2	**Программы-ревизоры, программы – фильтры** Назначение, принцип действия программ-ревизоров. Назначение, принцип действия программы-фильтров.		2
	3	**Профилактика заражения вирусом** Создание архивных копий информации и дискет с программными продуктами. Разграничение доступа к данным. Защита дискет от записи. Использование для перезагрузки компьютера с дискеты только защищенной		3

[3] в т.ч. 1 час консультаций

		от записи эталонной дискетой с операционной системой. Использование резидентных программ-фильтров для защиты от вирусов. Проверка целостности программ и данных каждый раз в начале работы с компьютером.		
	Практические занятия		2	
	1	Установка и настройка антивирусных программ		
	Самостоятельная работа обучающихся: - Изучение материала, вынесенного на самостоятельную проработку: Удаленная настройка антивирусных программ - Оформление отчета по практическим работам		4[4]	
Раздел 3. Организационно-правовое обеспечение информационной безопасности			8	
Тема 3.1. Международные, российские и отраслевые правовые документы	**Содержание**		4	
	1	**Правовое регулирование информационной безопасности в России** Опыт законодательного регулирования информатизации в России и за рубежом. Концепция правового обеспечения информационной безопасности Российской Федерации.	4	1
	2	**Система информационной безопасности в РФ. Разработка должностных инструкций** Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.		2
Тема 3.2.	**Содержание**		4	

[4] в т.ч. 1 час консультаций

Международные правовые акты в области информационной безопасности	1	**Международный опыт в области информационной безопасности** Основные тенденции международно-правового регулирования института защиты персональных данных. Международные правовые акты по защите информации.	2	1
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Простейшие шифры и их свойства		2	
		Всего:	72	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия кабинета архитектуры электронно-вычислительных машин и вычислительных систем.

Оборудование кабинета:
- стол преподавателя – 2 шт.
- стол аудиторный двухместный – 9 шт.
- стулья аудиторные – 30 шт.
- компьютерные столы – 10 шт.
- доска аудиторная для написания мелом – 1 шт.
- стеллаж – 1 шт.
- тумба – 1шт.
- сейф несгораемый – 1 шт.
- шкаф – 1 шт.
- стул преподавателя деревянный – 2 шт.
- стул мягкий – 1 шт.
- комплект учебно-наглядных пособий по дисциплине;

Технические средства обучения:
- персональный компьютер в сборе - 10 шт.
- проектор мультимедийный Sanyo PLC-XW50 - 1 шт
- экран проекционный Projecta - 1шт.
- МФУ лазерное Canon i-sensys MF 4018 - 1 шт.
- МФУ лазерное Canon i-sensys MF 4410 - 1 шт.
- демонстрационные дискеты, демонстрационные электронные платы, демонстрационные жесткие диски, CD-ROM, модем, сетевое оборудование локальной сети.

Программное обеспечение:
- Microsoft Windows XP Professional Open License: 47818817;
- Microsoft Office Professional Plus 2007 Open Li-cense:43219389;
- 7-Zip Свободная лицензия GNU LGPL;
- Adobe Acrobat Reader DC Бесплатное программное обеспечение;
- Mozilla Firefox Свободное программное обеспечение GNU GPL и GNU LGPL;
- Google Chrome Свободная лицензия BSD.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.— ЭБС «IPRbooks», по паролю

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; отв. ред. Т. А. Полякова, А. А. Стрельцов. — М. : Издательство Юрайт, 2017. — 325 с. — (Серия : Профессиональное образование). — ISBN 978-5-534-00843-2. — Режим доступа: http://www.biblio-online.ru- ЭБС «Юрайт».

Дополнительные источники:

1. Кодекс Российской Федерации об административных правонарушениях [Электронный ресурс] / . — Электрон. текстовые данные. — : Электронно-библиотечная система IPRbooks, 2017. — 567 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/1249.html

2. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 212 с. — 978-5-9963-0237-6. — Режим доступа: http://www.iprbookshop.ru/52182.html

3. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — 978-5-94774-821-5. — Режим доступа: http://www.iprbookshop.ru/52209.html

4. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс] / С.М. Авдошин, А.А. Савельева, В.А. Сердюк. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 с. — 978-5-4487-0147-4. — Режим доступа: http://www.iprbookshop.ru/72341.html

5. Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. — Электрон. текстовые данные. — Саратов: Ай Пи Ар Букс, 2015. — 326 с. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

6. Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 г. №149- ФЗ «Об информации, информационных технологиях и защите информации» (постатейный) [Электронный ресурс] / А.И. Савельев. — Электрон. текстовые данные. — М. : Статут, 2015. — 320 с. — 978-5-8354-1150-4. — Режим доступа: http://www.iprbookshop.ru/49072.html

Интернет-ресурсы:

1. Федеральный портал «Российское образование», предметный раздел: Информационная безопасность и защита компьютерной информации: http://www.edu.ru/
2. Лекции по дисциплине: http://protect.htmlweb.ru/p01.htm
3. Лекции по информационной безопасности, защите информации: http://all-ib.ru/
4. Официальный сайт журнала «Информационная безопасность»http://www.itsec.ru/news.php

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения: – определять необходимый уровень безопасности информации; – распознавать воздействие вируса на программный продукт или данные; – противодействовать вирусной атаке; – использовать антивирусные программы; *Знания:* – виды объектов, подлежащих защите, необходимость защиты информации; – источники и пути реализации несанкционированного доступа к информации; – уровни информационной безопасности объектов; – виды и назначение различных мер обеспечения информационной безопасности; – особенности использования технических и программно-математических мер; – назначение и место использования идентификации и аутентификации; – необходимость использования разграничения доступа; – основные возможности криптографических методов защиты информации; – пути проникновения компь-	*Оценка выполнения практических работ.* *Оценка защиты докладов, презентаций.* *Оценка выполнения индивидуальных заданий.* *Оценка результатов тестовых заданий* *Оценка ответов при проведении семинара* *Оценка выполнения индивидуальных заданий.* *Оценка результатов контрольной работы.* *Дифференцированный зачет*

ютерных вирусов; – классификацию деструктивных воздействий вируса; – средства защиты от воздействия вирусов; – виды и назначение антивирусных программ; – методы профилактики заражения вирусами; – основные международные правовые акты по защите информации; – основные положения и принципы международных соглашений; – соответствие российских и международных правовых соглашений; – российские общегосударственные правовые документы по защите информации; – российские отраслевые нормативные документы по защите информации; – назначение должностных инструкций; – методы контроля за исполнением должностных инструкций.	

РЕЦЕНЗИЯ

на рабочую программу учебной дисциплины «Информационная безопасность» для специальности 09.02.05 Прикладная информатика (по отраслям), составленную преподавателем И.Б. Ефимцевой

Рабочая программа разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.05 Прикладная информатика (по отраслям), утвержденным приказом Министерства образования и науки РФ от 13.08.2014 г. № 1001.

Структура рабочей программы соответствует Разъяснениям по формированию примерных программ учебных дисциплин начального профессионального и среднего профессионального образования на основе Федеральных государственных образовательных стандартов начального профессионального и среднего профессионального образования, утвержденным Директором Департамента государственной политики в образовании Министерства образования и науки Российской Федерации И.М. Реморенко от 27 августа 2009 г.

Рабочая программа учебной дисциплины состоит из 4 разделов:

- паспорта рабочей программы учебной дисциплины;
- структуры и содержания учебной дисциплины;
- условий реализации учебной дисциплины;
- контроля и оценки результатов освоения учебной дисциплины.

В паспорте рабочей программы учебной дисциплины определены область применения учебной дисциплины, место учебной дисциплины в структуре ППССЗ, цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины; отведенное количество часов на освоение учебной дисциплины.

Преподавателем составлен тематический план и содержание учебной дисциплины, определены условия реализации учебной дисциплины, включающие:

-требования к минимальному материально-техническому обеспечению

-информационное обеспечение обучения (перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы).

В соответствии с программой максимальная учебная нагрузка обучающегося составляет 72 часов, в том числе: обязательная аудиторная нагрузка- 48 часов, самостоятельная работа обучающихся- 24 часа.

В целом рецензируемая программа учебной дисциплины ориентирована на формирование общих и профессиональных компетенций, а так же на подготовку обучающихся к использованию полученных знаний и умений в своей профессиональной деятельности.

Таким образом, данная рабочая программа учебной дисциплины «Информационная безопасность» может быть рекомендована для применения в учебном процессе по специальности 09.02.05 Прикладная информатика (по отраслям).

Рецензент:
Зам. генерального директора
ООО «Армакс» _____ С.П. Николаенко
(подпись)

М.П.

Дата _____31.08.2016 г._____

РЕЦЕНЗИЯ

на рабочую программу учебной дисциплины «Информационная безопасность» для специальности 09.02.05 Прикладная информатика (по отраслям), составленную преподавателем И.Б. Ефимцевой

Настоящая рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.05 Прикладная информатика (по отраслям), утвержденным приказом Министерства образования и науки РФ от 13.08.2014 г. № 1001.

В программе определены область применения, место учебной дисциплины в структуре ППССЗ, цели и задачи учебной дисциплины, требования к результатам освоения дисциплины.

Рабочая программа закладывает основы знаний о видах объектов, подлежащих защите, о необходимости защиты информации.

Использование данной рабочей программы формирует у обучающихся представление об уровнях информационной безопасности объектов, видах и назначении различных мер обеспечения информационной безопасности.

Помимо этого, обучающиеся в процессе освоения дисциплины приобретают навыки распознавания воздействия вируса на программный продукт или данные.

Программа рассчитана на 72 максимальных часов, из них обязательная аудиторная нагрузка составляет 48 часов, и 24 часа отдается на самостоятельную работу.

Преподавателем составлен тематический план и содержание учебной дисциплины, определены условия реализации учебной дисциплины, включающие:

-требования к минимальному материально-техническому обеспечению;

-информационное обеспечение обучения (перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы).

Рабочая программа учебной дисциплины ориентирована на формирование общих и профессиональных компетенций, а так же на подготовку обучающихся к использованию полученных знаний и умений в своей профессиональной деятельности.

Данная рабочая программа учебной дисциплины «Информационная безопасность» может быть рекомендована для применения в учебном процессе по специальности 09.02.05 Прикладная информатика (по отраслям).

Рецензент:
преподаватель ФГБОУ ВО
«Курский государственный университет»,
колледж коммерции, технологий и сервиса _____ Негребецкая В.И.
(подпись)

Дата 31.08.2016 г.

АННОТАЦИЯ
рабочей программы учебной дисциплины
Информационная безопасность
по специальности
09.02.05 Прикладная информатика (по отраслям)
уровень подготовки - базовый
Квалификация техник-программист

1. Область применения программы:

Рабочая программа учебной дисциплины является частью ОПСПО ППССЗ в соответствии с ФГОС по специальности 09.02.05 Прикладная информатика (по отраслям). Рабочая программа учебной дисциплины может быть использована при разработке программ дополнительного профессионального образования в сфере экономической деятельности.

2. Место дисциплины в структуре основной профессиональной образовательной программы:

Дисциплина входит в общепрофессиональные дисциплины профессионального цикла.

3. Цели и задачи дисциплины - требования к результатам освоения дисциплины:

В результате изучения обязательной части цикла обучающийся должен:

уметь:

– определять необходимый уровень безопасности информации;
– распознавать воздействие вируса на программный продукт или данные;
– противодействовать вирусной атаке;
– использовать антивирусные программы;

знать:

– виды объектов, подлежащих защите, необходимость защиты информации;
– источники и пути реализации несанкционированного доступа к информации;
– уровни информационной безопасности объектов;
– виды и назначение различных мер обеспечения информационной безопасности;
– особенности использования технических и программно-математических мер;
– назначение и место использования идентификации и аутентификации;
– необходимость использования разграничения доступа;
– основные возможности криптографических методов защиты информации;
– пути проникновения компьютерных вирусов;
– классификацию деструктивных воздействий вируса;
– средства защиты от воздействия вирусов;
– виды и назначение антивирусных программ;
– методы профилактики заражения вирусами;
– основные международные правовые акты по защите информации;
– основные положения и принципы международных соглашений;
– соответствие российских и международных правовых соглашений;
– российские общегосударственные правовые документы по защите информации;
– российские отраслевые нормативные документы по защите информации;
– назначение должностных инструкций;

– методы контроля за исполнением должностных инструкций.

4. Общие количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 72 часа, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 48 часов;

самостоятельной работы обучающегося 24 часа.

В рабочей программе представлены:

- результаты освоения учебной дисциплины;
- структура и содержание учебной дисциплины;
- условия реализации программы учебной дисциплины;
- контроль и оценка результатов освоения учебной дисциплины.

Содержание рабочей программы учебной дисциплины полностью соответствует содержанию ФГОС по специальности 09.02.05 Прикладная информатика (по отраслям) и обеспечивает практическую реализацию ФГОС в рамках образовательного процесса.

5. Вид промежуточной аттестации: дифференцированный зачет

Разработчик: И.Б. Ефимцева, преподаватель ФГБОУ ВО «Курский государственный университет», колледж коммерции, технологий и сервиса