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

Колледж коммерции, технологий и сервиса

УТВЕРЖДЕНО
протокол заседания
ученого совета от 07.04.2020 г., № 8

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Курск 2020

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 14 часов;
самостоятельной работы обучающегося 58 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)	72
Обязательная аудиторная учебная нагрузка (всего)	14
в том числе:	
лабораторные занятия	-
практические занятия	4
контрольные работы	-
Самостоятельная работа обучающегося (всего)	58
Подготовка рефератов, докладов; изучение материала, вынесенного на самостоятельную проработку; выполнение домашней контрольной работы; оформление отчетов по практическим работам	58
Итоговая аттестация в форме *дифференцированного зачета*	

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)	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. Основные понятия информационной безопасности** 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. Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации	2	1
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Информационная безопасность деятельности общества и ее основные положения - изучение материала, вынесенного на самостоятельную проработку: **Угрозы информационной безопасности** Классификация угроз информационной безопасности, источники возникновения и пути реализации. Определение требований к уровню обеспечения информационной безопасности	6	

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	2	2
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Области и сферы по обеспечению информационной безопасности Стратегии обеспечения информационной безопасности фирм - изучение материала, вынесенного на самостоятельную проработку: **Специфические приемы управления техническими средствами** Приемы управления техническими средствами **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		8	
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.	2	
	Практические занятия		2	
	1	Защита информации в компьютерной системе от случайных угроз		
	Самостоятельная работа обучающихся: - оформление отчета по практической работе; - подготовка рефератов, докладов по темам: Способы шифрования Оформление отчета по практическим работам - изучение материала, вынесенного на самостоятельную проработку: **Основные возможности криптографических методов защиты информации**		8	

	Контроль целостности. Криптографические механизмы конфиденциальности, целостности и аутентичности информации **Обнаружение и противодействие атакам** Системы обнаружения атак на уровне сети. Обнаружение и противодействие информационным атакам из Интернета. Системы обнаружения беспроводных атак, принципов их работы и места в комплексе средств обеспечения безопасности беспроводной сети.		
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	2	2
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Модели защиты при отказе в обслуживании История криптографической деятельности - изучение материала, вынесенного на самостоятельную проработку: **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 **Программы-шпионы. Взлом парольной защиты** Программные закладки. Классификация программных закладов по методы их вне-	20	

	дрения. Группы деструктивных действий, которые могут осуществляться 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. **Средства защиты от воздействия вирусов** Защита от воздействия вирусов		
Тема 2.2. Классификация антивирусных программ	**Содержание**	12	
	Практические занятия	2	
	1 Установка и настройка антивирусных программ		
	Самостоятельная работа обучающихся: - Изучение материала, вынесенного на самостоятельную проработку: Удаленная настройка антивирусных программ **Программы-детекторы, программы-доктора** Назначение, классификация, недостатки, принцип действия программ-детекторов. Назначение, принцип действия программ-доктора. **Программы-ревизоры, программы – фильтры** Назначение, принцип действия программ-ревизоров. Назначение, принцип действия программы-фильтров. **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 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 - Оформление отчета по практическим работам	10	
Раздел 3. Органи-		8	

зационно-правовое обеспечение информационной безопасности			
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.	2	1
	Самостоятельная работа обучающихся: - Изучение материала, вынесенного на самостоятельную проработку: **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. Международные правовые акты в области информационной безопасности	**Содержание**	4	
	Самостоятельная работа обучающихся: - подготовка рефератов, докладов по темам: Простейшие шифры и их свойства - Изучение материала, вынесенного на самостоятельную проработку: **Международный опыт в области информационной безопасности** Основные тенденции международно-правового регулирования института защиты персональных данных. Международные правовые акты по защите информации.	4	
	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. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — М.: Юрайт, 2020. — 342 с.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — М.: Юрайт, 2020. — 325 с.

Дополнительные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — М.: Юрайт, 2020. — 161 с.

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.	