Министерство образования и науки Республики Татарстан
Государственное автономное профессиональное образовательное учреждение
«Камский строительный колледж имени Е.Н. Батенчука»

Рабочая программа учебной дисциплины

ОП.14 Информационная безопасность

по специальности
09.02.05 Прикладная информатика (по отраслям)

2019

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования 09.02.05 Прикладная информатика (по отраслям)

Рассмотрена
цикловой комиссией
естественнонаучных дисциплин
Протокол № 1
от «10» сентября 2019г.
ПЦК _____ Г.М. Габидинова

Утверждаю
Заместитель директора
по учебной работе
_____ Е.А. Закиуллина

«10» сентября 2019г.

Согласована
Начальник учебно - методического
отдела
_____ Г.М. Габидинова

«10» сентября 2019г.

Разработчик: преподаватель Гатина Т.Ф.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.05 Прикладная информатика (по отраслям).

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы: дисциплина входит в профессиональный цикл, относится к общепрофессиональным дисциплинам.

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

В результате изучения учебной дисциплины обучающийся должен показать **формирование профессиональных и общих компетенций:**

ПК 1.4. Настраивать и работать с отраслевым оборудованием обработки информационного контента

ПК 1.5. Контролировать работу компьютерных, периферийных устройств и телекоммуникационных систем, обеспечивать их правильную эксплуатацию.

ПК 2.3. Проводить отладку и тестирование программного обеспечения отраслевой направленности.

ПК 2.4. Проводить адаптацию отраслевого программного обеспечения.

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-коммуникационные технологии в профессиональной деятельности.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

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

- *выполнять анализ способов нарушений информационной безопасности;*
- *использовать методы и средства защиты данных;*
- *выбирать формы и критерии информационной безопасности;*
- *разрабатывать предложения по совершенствованию политики безопасности;*
- *шифровать хранимые и передаваемые данные;*
- *применять оптимальные типы криптографических протоколов при передаче информации;*
- *применять компьютерные средства защиты информации от несанкционированного доступа.*

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

- *свойства информации, определяющие выбор средств и методов информационной защиты и влияющие на ее результативность,*
- *основное содержание, средства и методы используемых на практике или используемых на практике или развиваемых направлений информационной защиты,*
- *основные принципы, стратегии и модели информационной защиты, основные принципы, стратегии и модели информационной защиты,*

- наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий, и типичные качества

личности преступников, -

- составы преступлений в сфере компьютерной информации и толкование специальных терминов, употребляемых в них,

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;

-виды угроз информационной безопасности;

- методы и средства обеспечения информационной безопасности компьютерных систем;

- существующие стандарты информационной безопасности;

- принципы комплексирования средств и методов защиты информации.

1.4. Количество часов на освоение рабочей программы учебной дисциплины:

максимальной учебной нагрузки обучающегося - **60** часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося - **40** часов;

самостоятельной работы обучающегося - **20** 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)	***60***
Обязательная аудиторная учебная нагрузка (всего)	***40***
в том числе:	
практические занятия (всего):	***10***
Самостоятельная работа обучающегося (всего):	***20***
Итоговая аттестация в форме дифференцированного ***зачета***	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся		Объем часов	*Уровень освоения*
1	*2*		*3*	4
Раздел 1. Борьба с угрозами несанкционированного доступа			**27**	
Тема 1.1 Актуальность проблемы обеспечения информационной безопасности	**Содержание учебного материала**			
	1	Основные понятия объекты, цели и задачи информационной безопасности**.** Основные понятия информационной безопасности.	2	2
	2	Угрозы информационной безопасности: классификация, источники возникновения	2	2
	Практические занятия		2	
	1	Составление схемы информационных потоков на исследуемом объекте.		
	Самостоятельная работа обучающегося		3	
	Подготовить презентацию на тему «Действия и события, нарушающие информационную безопасность»			
Тема 1.2 Виды мер обеспечения информационной безопасности	**Содержание учебного материала**			
	1	Виды мер обеспечения информационной безопасности.	2	2
	2	Мероприятия по защите информации.	2	2
	3	Виды и характеристики современных средств защиты.	2	2
	4	Аспекты, относящиеся к средствам защиты: аппаратные ключи, лицензирование, метод авторизации	2	2
	Практические занятия			
	1	Управление шаблонами безопасности в	2	
	2	Настройка параметров аутентификации	2	
	Самостоятельная работа обучающегося		6	
	Подготовить презентацию на тему “Современные технические средства защиты информации”			
Раздел 2. Борьба с вирусным заражением			**21**	
Тема 2.1 Проблема вирусного заражения и структура современных вирусов	**Содержание учебного материала:**			
	1	Общая характеристика компьютерных вирусов. Классификация компьютерных вирусов.	2	2
	2	Признаки проявления вирусов. Структура вирусов, пути их распространения.	2	2

	3	Кейлоггеры. Классификация по типу, по месту хранения, по методу отправки и методу применения.	2	2
	4	Модели поведения вирусов и их деструктивные действия	2	2
	Самостоятельная работа обучающегося		4	
	Подготовить презентацию на тему “Компьютерный вирус ”			
Тема 2.2 Защита от воздействия вирусов	**Содержание учебного материала:**			
	1	Классификация методов защиты от компьютерных вирусов. Виды и назначение антивирусных программ	2	2
	2	Состав программного комплекса защиты от вирусов. Общая характеристика средств нейтрализации компьютерных вирусов.	2	2
	Практические работы		2	
	1	Обзор современных антивирусных программ		
	Самостоятельная работа обучающегося		3	
	Подготовить презентацию на тему “Антивирусная программа ”			
Раздел 3. Организационно-правовое обеспечение информационной безопасности			**12**	
Тема 3.1 Международные, российские и отраслевые правовые документы	**Содержание учебного материала:**			
	1	История становления Российского законодательства в области информационной безопасности, основные нормативные акты.	2	2
	2	Международные правовые акты по защите информации.	2	2
	Практические работы		2	
	1	Нормативно-правовая база информационной безопасности		
	Дифференцированный зачет		2	2
	Самостоятельная работа обучающегося		4	
	Подготовить презентацию на тему «Нормативно-правовая база РФ и статьи Уголовного кодекса РФ, регулирующие вопросы информационной безопасности»			
	Всего:		**60**	

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 УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к материально-техническому обеспечению

Для реализации учебной дисциплины имеется в наличии лаборатория обработки информации отраслевой направленности.

Оборудование лаборатории:
- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-методической документации

Технические средства обучения:
- персональный компьютер;
- проекционный экран;
- мультимедийный проектор;
- доска;
- колонки

3.2.Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Ищейнов В. Я. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2018. - 208 с. [ЭБС www.znanium.com].
2. Партыка Т. Л. Информационная безопасность: Учебное пособие/Партыка Т. Л., Попов И. И., 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2019. - 432 с. [ЭБС www.znanium.com].

Дополнительные источники:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2019. - 416 с. [ЭБС www.znanium.com].
2. Васильков А. В. Безопасность и управление доступом в информационных системах : учеб. пособие / А.В. Васильков, И.А. Васильков. — М. : ФОРУМ : ИНФРА-М, 2019. — 368 с. — (Среднее профессиональное образование). [ЭБС www.znanium.com].

Интернет-ресурсы:

1. Начало программирования. Форма доступа: http:www.pas1. ru
2. Компьютерные видео уроки. Форма доступа: http://compteacher.ru/programming/delphi
3. Книги по программированию. Форма доступа: http://delphi-z.ru/books.html
4. Программирование на Visual Basic. Форма доступа: http://vbnet.ru/articles/showarticle.aspx?id=99
5. http://informatics.wallst.ru/ - любая информация о программировании
6. http://www.ugatu.ac.ru/~trushin - методических материалов по информатике
7. Андерс Хейлсберг. Языки программирования, учебники и уроки http://program-yaziki.ucoz.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (формирование профессиональных компетенций ПК 1.4, 1.5, 2.3, 2.4, освоенные умения, усвоенные знания, развитие общих компетенций ОК1 –ОК5, ОК9)	Формы и методы контроля и оценки результатов обучения
Профессиональных компетенций:	
ПК 1.4. Настраивать и работать с отраслевым оборудованием обработки информационного контента ПК 1.5. Контролировать работу компьютерных, периферийных устройств и телекоммуникационных систем, обеспечивать их правильную эксплуатацию. ПК 2.3. Проводить отладку и тестирование программного обеспечения отраслевой направленности. ПК 2.4. Проводить адаптацию отраслевого программного обеспечения.	Оценка результатов выполнения и защиты лабораторных и практических работ; Оценка результатов выполнения внеаудиторной самостоятельной работы; Тестирование; Дифференцированный зачет.
Умения:	
- выполнять анализ способов нарушений информационной безопасности; *- использовать методы и средства защиты данных;* *- выбирать формы и критерии информационной безопасности;* *- разрабатывать предложения по совершенствованию политики безопасности;* *- шифровать хранимые и передаваемые данные;* *- применять оптимальные типы криптографических протоколов при передаче информации;* *- применять компьютерные средства защиты информации от несанкционированного доступа.*	
Знания *- свойства информации, определяющие выбор средств и методов информационной защиты и влияющие на ее результативность* *- основные принципы, стратегии и модели информационной защиты, основные принципы, стратегии и модели информационной защиты,* *- наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий, и типичные качества личности преступников* *место и роль информационной безопасности в системе национальной безопасности Российской Федерации;* *- виды угроз информационной безопасности;* *методы и средства обеспечения информационной безопасности компьютерных систем;* *существующие стандарты информационной безопасности;* *принципы комплексирования средств и методов защиты информации.*	
Общие компетенции:	

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-коммуникационные технологии в профессиональной деятельности. ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	Интерпретация результатов Наблюдений за деятельностью Обучающегося в процессе освоения образовательной программы