Приложение 3.7.11.

Федеральное казенное образовательное учреждение
«Кинешемский технологический техникум-интернат»
Министерства здравоохранения и социального развития Российской Федерации

Рассмотрено
на заседании ЦМК
ОПД спец-м пр-е в к.с.
Протокол № 1
от «31» августа 2016 г.
Председатель ЦМК
(Никитина С.Б.)

Утверждено
Зам.директора по учебной работе
Н.П.Векшинская
«30» 08 2016 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

для специальности СПО 09.02.03 Программирование в компьютерных системах

2016 г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.03 Программирование в компьютерных системах.

Организация-разработчик:

Федеральное казённое профессиональное образовательное учреждение среднего профессионального образования «Кинешемский технологический техникум – интернат» Министерства труда и социальной защиты Российской Федерации (ФКПОУ «КТТИ» Минтруда России)

Разработчик:

Галкин И. Ю., преподаватель, ФКПОУ «КТТИ» Минтруда России.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

1.1. Область применения рабочей программы (далее программа)

Программа учебной дисциплины является частью адаптированной образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.03 Программирование в компьютерных системах.

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы: дисциплина входит в вариативную часть профессионального цикла.

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

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

- анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ;
- ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ;
- применять правовые, организационные, технические и программные средства защиты информации.

В результате освоения учебной дисциплины студент ***должен знать***:

- основы информационной безопасности и защиты информации;
- принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа;
- источники возникновения информационных угроз;
- методы антивирусной защиты информации;
- законодательную и нормативную базу ИБ.

1.3.1 Изучение учебной дисциплины направлено на формирование у обучающихся общих (ОК) и профессиональных (ПК) компетенций (из ФГОС, таблица «Структура программы подготовки специалистов среднего звена)**:**

ОК 1 - 9

ПК 1.1, 1.2, 2.4, 3.4.

1.4. Количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки студента 87 часов, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося 58 часа;
- самостоятельной работы студента 29 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)	**87**
Обязательная аудиторная учебная нагрузка (всего)	**58**
в том числе:	
практические занятия	16
Самостоятельная работа обучающегося (всего)	**29**
в том числе:	
Проработка конспектов занятий, специальной технической литературы (по вопросам, составленным преподавателем).	14
выполнение домашних и индивидуальных заданий	15
Итоговая аттестация в форме экзамена	

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Актуальность проблемы обеспечения безопасности информации.			
Тема 1.1 Основные понятия безопасности.	**Содержание учебного материала**	8	1
	Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Классификация угроз информационной безопасности. Угрозы информационной безопасности: источники возникновения и пути реализации.		
	Самостоятельная работа: выполнение домашних заданий по разделу 1. Проработка конспектов занятий, специальной технической литературы (по вопросам, составленным преподавателем).	4	3
Раздел 2. Меры обеспечения информационной безопасности.			
Тема 2.1 Виды мер обеспечения информационной безопасности	**Содержание учебного материала**	6	1
	Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Достоинства и недостатки различных видов мер защиты.		
Тема 2.2 Методы защиты от копирования	**Содержание учебного материала**	6	1
	Методы защиты от копирования. Некопируемые метки. Защита от средств отладки и дисассемблирования. Защита от трассировки по заданному прерыванию. Защита программ в оперативной памяти.		
	Самостоятельная работа: выполнение домашних заданий по разделу 2, индивидуальных заданий. Проработка конспектов занятий, специальной технической литературы (по вопросам, составленным преподавателем). **Тематика внеаудиторной самостоятельной работы** 1. Подготовка презентации на тему «Угрозы информационной безопасности».	6	3
Раздел 3 Защита информации от несанкционированного доступа			
Тема 3.1 Средства и	**Содержание учебного материала**	4	2

механизмы защиты информации от несанкционированного доступа.	Основные защитные механизмы: идентификация и аутентификация. Контроль целостности. Разграничение доступа.		
Тема 3.2 Криптография.	**Содержание учебного материала**	2	1
	Основные понятия. Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Цифровая подпись. Криптографические средства защиты. Криптосистемы. Методология с использованием ключа.		
	Практические занятия 1. Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Цифровая подпись. 2. Методология с использованием ключа.	2	3
	Самостоятельная работа: выполнение домашних заданий по разделу 3. Проработка конспектов занятий, специальной технической литературы (по вопросам, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя. **Тематика внеаудиторной самостоятельной работы** 1. Методы взлома компьютерных систем. 2. Настройка политики учетных записей. 3. Настройка параметров безопасности операционных систем.	4	
Раздел 4. Антивирусная защита информации.			
Тема 4.1 Компьютерные вирусы	**Содержание учебного материала**	8	2
	Компьютерный вирус: понятие, пути распространения. Классификация вирусов. Проявление действия вируса. Структура современных вирусов. Модели поведения вирусов. Деструктивные действия вируса; разрушение программы защиты. Изменение состояния программной среды. Воздействия на программно-аппаратные средства защиты информации.		
	Практические занятия 3. Классификация вирусов. 4. Проявление действия вируса. 5. Деструктивные действия вируса; разрушение программы защиты. 6. Воздействия на программно-аппаратные средства защиты информации.	8	
Тема 4.2 Защита от воздействия вирусов.	**Содержание учебного материала**	6	2
	Защита от воздействия вирусов. Антивирусные программы. Программы-шпионы. Взлом парольной защиты. Программы–детекторы, программы–доктора, программы–ревизоры. Профилактика заражения вирусом.		

	Практические занятия 7. Программы-шпионы. Взлом парольной защиты. 8. Программы–ревизоры. 9. Профилактика заражения вирусом.	6	3
	Самостоятельная работа: выполнение домашних заданий по разделу 4. Проработка конспектов занятий, специальной технической литературы (по вопросам, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя. **Тематика внеаудиторной самостоятельной работы** 1. Современные пакеты антивирусных программ. Их характеристика и возможности применения. 2. Приемы работы с антивирусным программным обеспечением. 3. Основные способы защиты от потери информации и нарушений 4. работоспособности вычислительных средств. 5. Способы резервировании информации. 6. Реферат на тему: Пути проникновения компьютерных вирусов. 7. Антивирусное программное обеспечение и его классификация.	14	3
Раздел 5. Организационно – правовое обеспечение информационной безопасности.			
Тема 5.1 Правовое обеспечение информационной безопасности.	**Содержание учебного материала** Опыт законодательного регулирования информатизации в России и за рубежом. Концепция правового обеспечения информационной безопасности Российской Федерации. Состав и назначение должностных инструкций.	2	1
	Самостоятельная работа: выполнение домашних заданий по разделу 5. Проработка конспектов занятий, специальной технической литературы (по вопросам, составленным преподавателем). **Тематика внеаудиторной самостоятельной работы** 1. Изучение опыта законодательного регулирования информатизации за рубежом	1	3
	Всего:	**87**	

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 минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета.

Оборудование учебного кабинета:

1. посадочные места по количеству обучающихся;
2. рабочее место преподавателя;
3. комплект сетевого оборудования, обеспечивающий соединение всех компьютеров, установленных в кабинете в единую сеть, с выходом в Интернет;
4. аудиторная доска для письма;
5. компьютерные столы по числу рабочих мест обучающихся;

Технические средства обучения:

1. мультимедиапроектор;
2. персональные компьютеры с лицензионным программным обеспечением;
3. лазерный принтер;
6. устройства вывода звуковой информации.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования 2-е издание М.: Издательский центр «Академия», 2016 г

Интернет-ресурсы:

1. Интернет-Университет информационных технологий (Интуит)-Национальный открытый университет. Библиотека учебных курсов [Электронный ресурс]. - Режим доступа: http://old.intuit.ru, свободный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения – анализировать и выбирать адекватные модели информационной безопасности, планировать их реализацию на базе требований к современному уровню ИБ; – ориентироваться в инфраструктуре проекта по разработке и внедрению средств, реализующих ИБ; – применять правовые, организационные, технические и программные средства защиты информации. Знания – основы информационной безопасности и защиты информации; – принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа; – источники возникновения информационных угроз; – методы антивирусной защиты информации; – законодательная и нормативная база ИБ.	1. Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. 2. Текущий контроль в форме: - практических работ; - тестирования; - домашней работы; - отчёта по проделанной внеаудиторной самостоятельной работе (представление реферата, презентации, информационное сообщение). 3. Итоговая аттестация в форме экзамена.