МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Колледж радиоэлектроники имени П.Н. Яблочкова

УТВЕРЖДАЮ
_____
"15" июля 2020г.

Рабочая программа учебной дисциплины

Информационная безопасность

09.02.07 Информационные системы и программирование

Профиль подготовки
технологический
Квалификация выпускника
программист
Форма обучения
очная

Саратов

2020

Разработчики: преподаватель В.С. Белицкая

Рассмотрено на заседании ЦК программирования, информатики и вычислительной техники

от «25» 05 2020 г. Протокол № 9

Председатель ЦК программирования, информатики и вычислительной техники _____ Е.Д.Шаманаева

Директор Колледжа радиоэлектроники имени П.Н. Яблочкова О.В.Бреус

Заместитель директора по УР Н.Н.Чернова

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование.

Организация- разработчик: ФГБОУ ВО «СГУ имени Н.Г. Чернышевского» Колледж радиоэлектроники имени П.Н. Яблочкова СГУ.

Разработчик: Белицкая В.С. - преподаватель Колледжа радиоэлектроники имени П.Н. Яблочкова СГУ.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена: дисциплина относится к общепрофессиональному циклу.

1.3. Цель и планируемые результаты освоения дисциплины:

В результате освоения учебной дисциплины обучающийся должен уметь:

— применять правовые, организационные, технические и программные средства защиты информации;

— создавать программные средства защиты информации.

В результате освоения учебной дисциплины обучающийся должен знать:

— источники возникновения информационных угроз;

— модели и принципы защиты информации от несанкционированного доступа;

— методы антивирусной защиты информации;

— состав и методы организационно-правовой защиты информации.

ПК и ОК, которые актуализируются при изучении учебной дисциплины:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Планировать предпринимательскую деятельность в профессиональной сфере.

ПК 1.1. Формировать алгоритмы разработки программных модулей в соответствии с техническим заданием.

ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

1.4 Количество часов на освоение программы дисциплины:

учебной нагрузки обучающегося 78 часов, в том числе:

учебной нагрузки обучающегося во взаимодействии с преподавателем 60 часов;

самостоятельной учебной работы обучающегося 10 часов.

промежуточная аттестация 8 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объём в часах
учебной нагрузки обучающегося	78
учебная нагрузка во взаимодействии с преподавателем	60
в том числе:	
теоретическое обучение	38
практические занятия	22
Самостоятельная учебная работа обучающегося	10
Промежуточная аттестация в форме экзамена	

Тематический план и содержание учебной дисциплины информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект).	Объем часов	Уровень освоения
1	2	3	4
Введение	Роль дисциплины в становлении специалистов. Взаимосвязь дисциплин.	2	
Раздел 1 Информационная безопасность. Общие понятия и определения.		4	
Тема 1.1 Информационная безопасность. Общие понятия и определения.	Содержание	2	1
	Актуальность информационной безопасности. Свойства информации, влияющие на информационную безопасность.	2	
Тема 1.2 Компьютерные преступления	Содержание	2	1
	Классификация компьютерных преступлений и способы их совершения. Причины уязвимости сети интернет.	2	
Раздел 2 Вредоносные программы и защита от компьютерных вирусов.		12	
Тема 2.1. Классификация компьютерных вирусов.	Содержание	4	1
	Условия существования вирусов. Классификация компьютерных вирусов. Классические компьютерные вирусы. Компьютерные черви и троянские программы.	4	
Тема 2.2 Защита от компьютерных вирусов.	Лабораторные занятия	8	2
	Лабораторная работа №1 Макровирусы и борьба с ними в MS Office. *Лабораторная работа №2 Профилактика проникновения «Троянских программ».* *Лабораторная работа №3 Антивирус Касперского. Настройка и поиск вирусов.*	8	
Раздел 3 Методы и средства защиты компьютерной информации.		8	
Тема 3.1. Защита информации. Основные принципы.	Содержание	4	1
	Понятие защиты информации. Основные принципы защиты информации.	*4*	

Тема 3.2. Методы и средства защиты информации.	Содержание	4	1
	Методы и средства защиты информации. Разграничение прав пользователей. Регистрация всех обращений к информации, защита от копирования.	4	
Раздел 4 Криптографические методы защиты информации		28	
Тема 4.1. Основные этапы развития криптологии.	Содержание	2	
	Криптология и основные этапы ее развития.	2	
Тема 4.2. Классификация методов криптографического закрытия информации	Содержание	14	1
	Шифрование заменой. Криптоанализ. Основные понятия. Шифрование методом перестановки и гаммированием. Шифрование с помощью аналитических преобразований.	4	
	Лабораторные занятия	10	2
	Лабораторная работа №5 Шифрование методом замены *Лабораторная работа №6 Криптоанализ по оценке частотности символов.* *Лабораторная работа №7 Шифрование методом перестановки.* *Лабораторная работа №8 Шифрование методом гаммирования.*		
Тема 4.3. Системы с открытым ключом.	Содержание	8	1
	Принцип работы систем с отрытым ключом. Криптографические стандарты DES и ГОСТ 28147-89. Алгоритм RSA.	4	
	Лабораторные занятия	4	2
	Лабораторная работа №9 Шифрование с отрытым ключом. Алгоритм RSA/		
Тема 4.4 Проблемы реализации и характеристики криптографических средств защиты	Содержание	4	1
	Оценка криптостойкости шифров. Технико-экономические показатели криптографических методов защиты информации.	4	
Раздел 5 Правовое обеспечение информационной безопасности.		4	
Тема 5.1. Правовое обеспе-	Содержание	4	1

	Тематика внеаудиторной самостоятельной работы Подготовка рефератов и сообщений по темам: Классификация нарушителей. Знакомство с антивирусными программами. Основные методы криптоанализа. Преимущества и недостатки систем с отрытым ключом. Выбор средств защиты для собственной программы. Программно-аппаратная реализация средств защиты	10	
	Итоговое занятие	2	1
	Всего:	78	
	Промежуточная аттестация экзамен	8	8

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация программы дисциплины требует наличия лаборатории информационных ресурсов

Технические средства обучения: интерактивная доска с мультимедийным проектором, персональный компьютер для преподавателя, несколько рабочих станций для проверки знаний студентов.

Оборудование лаборатории и рабочих мест лаборатории: компьютерные рабочие станций для работы студентов.

3.2. Информационное обеспечение обучения

Перечень учебных изданий, интернет-ресурсов, дополнительной литературы

Основные источники:

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М: ИД «ФОРУМ»: ИНФРА–М., 2016. – 416 с.– (Профессиональное образование)

Рекомендовано Министерством образования РФ в качестве учебного пособия для студентов учреждений СПО, обучающихся по группе специальностей 2200 «Информатика и вычислительная техника».

2. Мельников В.П. Информационная безопасность: Учебное пособие для студ. сред. проф. образования /В.П.Мельников, С.А.Клейменов, А.М.Петраков, под ред. С.А.Клейменова. – 2-е изд. стер. – М: Издательский центр «Академия», 2017. – 336 с.

Допущено Министерством образования РФ в качестве учебного пособия для студентов учреждений СПО, обучающихся по группе специальностей 2200 «Информатика и вычислительная техника».

Дополнительные источники

1. Партыка Т. Л., Попов И. И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. — М.: ФОРУМ: ИНФРА-М, 2013. – 368 с.: ил. - (Серия «Профессиональное образование»).

Допущено Министерством образования РФ в качестве учебного пособия для студентов учреждений СПО, обучающихся по группе специальностей 2200 «Информатика и вычислительная техника».

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства /Шаньгин В.Ф. – М: ДМК Пресс, 2013. – 544 с.

Допущено учебно-методическим объединением ВУЗов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению230100 «Информатика и вычислительная техника».

2. Сычев Ю.Н. Основы информационной безопасности. Учебно-практическое пособие. – М.: Изд. центр ЕАОИ, 2014. – 300 с.

3. И.В. Аникин, В.И. Глова Методы и средства защиты компьютерной информации // Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2015 с. 417.

4. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. -М.: Горячая линия - Телеком, 2016. - 544 с: ил.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	Основные показатели оценки результата
применять правовые, организационные, технические и программные средства защиты информации; создавать программные средства защиты информации. источники возникновения информационных угроз; модели и принципы защиты информации от несанкционированного доступа; методы антивирусной защиты информации; состав и методы организационно-правовой защиты информации.	понимание правовых, организационных, технических и программных средств защиты информации, программных средств защиты информации. анализ источников возникновения информационных угроз; оценка модели и принципов защиты информации от несанкционированного доступа, методов антивирусной защиты информации; анализ состава и методов организационно-правовой защиты информации.