Министерство образования, науки и молодежи Республики Крым
Государственное бюджетное профессиональное образовательное учреждение
Республики Крым
«Симферопольский колледж радиоэлектроники»

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____В.И.Полякова
«30» 08 2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11 Защита информации

специальности
09.02.01 Компьютерные системы и комплексы

Симферополь
2019 г.

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Республики Крым «Симферопольский колледж радиоэлектроники»

Разработчик – преподаватель ГБПОУ РК «Симферопольский колледж радиоэлектроники»:

Сапрыкин Сергей Юрьевич_____

Утверждено на заседании ЦМК №5
протокол № 1
«27» 08 2019 г.
Председатель цикловой комиссии
_____С.Г. Мелихова

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Защита информации

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы: Данная дисциплина относится к общепрофессиональным дисциплинам профессионального цикла.

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

В результате освоения дисциплины обучающийся должен уметь:

- использовать различные технические средства в процессе обработки, хранения и передачи информации;
- определять возможные виды атак;
- классифицировать основные угрозы безопасности информации
- применять криптографические методы защиты информации;

В результате освоения дисциплины обучающийся должен знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих
- место информационной безопасности в системе национальной безопасности страны
- источники угроз информационной безопасности и меры по их предотвращению
- современные средства и способы обеспечения информационной безопасности

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 141 часов, в том числе:

аудиторной учебной работы обучающегося (обязательных учебных занятий) 94 часов;

внеаудиторной (самостоятельной) учебной работы обучающегося 47 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)	*141*
Аудиторная учебная работа (обязательные учебные занятия) (всего)	*94*
в том числе:	
лабораторные занятия	-
практические занятия	*40*
контрольные работы	-
курсовая работа (проект)	-
Внеаудиторная (самостоятельная) учебная работа обучающегося (всего):	*47*
– подготовка к зачету	*11*
– подготовка к практическому занятию	*18*
– оформление отчета	*18*
Промежуточная аттестация в форме дифференцированного зачета	

2.2. Тематический план и содержание учебной дисциплины Защита информации

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) *(если предусмотрены)*	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Концепция и основные направления обеспечения безопасности информационной безопасности		**4**	
Тема 1.1. Информационная безопасность. Классификация угроз	**Содержание учебного материала** 1. Понятие информационной безопасности. Международные стандарты информационного обмена. Понятие угрозы. Действия, приводящие к неправомерному овладению конфиденциальной информации. Виды противников «нарушителей». 2. Основные концептуальные положения системы защиты информации. Объекты, источники угроз. Классификация угроз. Направления обеспечения информационной безопасности	4	2
Раздел 2. *Обеспечение информационной безопасности*		**24**	
Тема 2.1. Правовое обеспечение информационной безопасности	**Содержание учебного материала** 1. Государственная политика информационной безопасности. Органы обеспечения информационной безопасности. Лицензирование деятельности в области информационной безопасности 2. Правовые акты, правила, процедуры и мероприятия, обеспечивающие правовую защиту информации	4	2
	Практические занятия Создание модели информационной безопасности	4	2
	Самостоятельная работа подготовка к выполнению практической работы, оформление отчета	4	
Тема 2.2. Организационное обеспечение информационной безопасности	**Содержание учебного материала** 1. Основные положения теории информационной безопасности информационных систем 2. Модели безопасности и их применение. Организационные мероприятия информационной безопасности	4	2
Тема 2.3 Технические средства обеспечения информационной безопасности	**Содержание учебного материала** 1. Классификация средств инженерно-технической защиты. Технические каналы утечки информации. 2. Классификация, выявление (поиск) технических каналов утечки информации. Индикаторы поля, интерсепторы и измерители частоты 3. Программно-аппаратные поисковые комплексы. Средства контроля двухпроводных линий. Методы и средства защиты информации от утечки по техническим каналам	6	2
Раздел 3. ***Основы криптографии***		**50**	
Тема 3.1. Традиционные системы шифрования	**Содержание учебного материала** 1. Перестановочные шифры. Шифр перестановки «скитала». Шифрующие таблицы. Применение магических квадратов. Шифрующие таблицы. Подстановочные шифры. Полибианский квадрат 2. Шифр Цезаря. Система шифрования Вижинера. Применение операции «исключающего или». Одноразовые блокноты. Простейшие потоковые шифры	6	2

	3. Самосинхронизирующиеся потоковые шифры. Синхронные потоковые шифры		
Тема 3.2. Современные симметричные криптосистемы	**Содержание учебного материала** 1. Применение принципов рассеивания и перемешивания. Схема Файстеля 2. Режимы использования симметричных шифров. Стандарт DES, 3DES	4	2
Тема 3.3. Ассиметричные криптосистемы	**Содержание учебного материала** 1. Безопасность алгоритмов с открытыми ключами. Алгоритм RSA. Алгоритм Полига – Хеллмена 2. Схема Рабина. Схема Вильямса. Схема Эль-Гамаля. Цифровые подписи по схеме Эль-Гамаля	4	2
Тема 3.4. Потоковые криптосистемы	**Содержание учебного материала** 1. Шифр SNOW. Стохастические поточные шифры 2. Синхронное и самосинхронизирующееся шифрование	4	
Тема 3.5. Цифровая подпись	**Содержание учебного материала** 1. Однонаправленные функции. Snefru. Message Digest(MD5) 2. Цифровая подпись DSS. Алгоритмы цифровой подписи DSA, RSA, ГОСТ	4	
Тема 3.6. Типовая архитектура подсистемы защиты операционной системы	**Содержание учебного материала** 1. Основные функции подсистемы защиты операционной системы Windows. Разграничение доступа к объектам операционной системы 2. Основные функции подсистемы защиты операционной системы Linux. Разграничение доступа к объектам операционной системы	4	2
Тема 3.7. Управление ключами и защищенные протоколы обмена персональными данными	**Содержание учебного материала** 1. Общий подход к использованию протоколов. Криптографические схемы разделения секрета. Концепция центра распределения ключей	2	2
Тема 3.8. Стеганография	**Содержание учебного материала** 1. Основные определения. Классификация систем стеганографии. Классификация систем встраивания цифровых водяных знаков. 2. Дифференцированный зачет	4	2
	Практические работы 1. Исследование стандарта криптографической защиты AES 2. Исследование системы криптографической защиты RSA 3. Исследование симметричного алгоритма криптосистемы ГОСТ-28410-89 4. Исследование стандартов хэш-функции и электронной цифровой подписи 5. Разграничение доступа в ОС Windows 6. Разграничение доступа в ОС Linux 7. Разграничение доступа с использованием межсетевых фильтров 8. Применение метода замены наименее значащего бита 9. Применение метода псевдослучайного интервала	36	2
	Самостоятельная работа подготовка к выполнению практической работы, оформление отчета, подготовка к зачету	43	
	Всего:	141	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническоме обеспечение

Реализация программы дисциплины требует наличия лабораторий «Информационной безопасности».

Технические средства обучения:

- ПЭВМ Intel Pentium на 15 мест с программным обеспечением
- мультимедиапроектор
- интерактивная доска
- локальная сеть и доступ с рабочих мест к ресурсам Internet.
- Программное обеспечение: операционная системаWindows/Linux, среда программирования Nenbeans

3.2. Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Мельников В.П., Клейменов С.А., Петраков А.В., «Информационная безопасность», под ред. С.А.Клейменова, 2013- 336 с.
2. Бубнов А.А. «Основы информационной безопасности»: учеб. пособие для студ. учреждений сред. проф. образования / Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. – М. : Издательский центр «Академия», 2015. -256с.
3. Емельянова Н.З. Партыка Т.Л. Попов И.И. «Защита информации в персональном компьютере» учебное пособие – М.Форум. 2013 -368с.
4. Шаньгин В. Ф. И Защита информации в компьютерных системах и сетях. / В.Ф. Шаньгин, Москва: ДМК Пресс, 2012. – 592 с.: ил.

Дополнительные источники:

1. Гордейчик С. В., Дубровин В. В. Безопасность беспроводных сетей. – М.: Горячая линия – Телеком, 2008. – 288 с.
2. Вишневский В. М., Портной С. Л., Шахнович И. В. Энциклопедия WiMAX. Путь к 4G. – М.: Техносфера, 2009. – 472 с.
3. Конахович Г.Ф. Пузыренко А.Ю. Компьютерная стеганография. Теория и практика, 2006 – 288с
4. http://www.infosecurity.ru/
5. http://www.void.ru/
6. http://www.jetinfo.ru/
7. http://www.infosec.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Основные показатели оценки результата**
Умения:	
Использовать различные технические средства в процессе обработки, хранения и передачи информации;	Защита отчетов по практическим работам, интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Определять возможные виды атак;	
Проводить оценку эффективности системы защиты;	
Производить установку и настройку средств защиты;	
Выполнять тестирование системы систем с целью определения уровня защищенности;	
Применять криптографические методы защиты информации;	
Знания:	
Нормативно-правовые и законодательные акты в области информационной безопасности	внеаудиторная самостоятельная работа
Назначение, классификацию и принципы работы, специализированного оборудования;	тестирование
Конфигурации защищаемых сетей	Защита отчетов по практическим работам, внеаудиторная самостоятельная работа
Принципы построения информационно-коммуникационных сетей;	

Собственные средства защиты различных операционных систем и сред	
Основные методы обеспечения информационной безопасности	Защита отчетов по практическим работам
Принцип построения систем защиты	тестирование
Каналы утечки информации	
Итоговая аттестация усвоенных знаний и освоенных умений	*Дифференцированный зачет*