МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ И РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)

Колледж экономики управления и права

УТВЕРЖДАЮ
Директор колледжа ЭУП
_____ В.И. Мигаль
личная подпись
«30» июня 2021 г

Рег. № _____

РАБОЧАЯ ПРОГРАММА

По дисциплине ОП.11 Информационная безопасность

По специальности 09.02.04 Информационные системы (по отраслям)
Форма и срок освоения ППССЗ: очная 3 г. 10 мес. нормативный
Максимальное количество учебных часов – 72 часа.
Всего аудиторных занятий – 48 часов.

Из них в семестре:

Лекции –	16 часов.
Практические занятия –	32 часа.
Всего часов на самостоятельную работу студента	18 часов
Консультации –	6 час

ФОРМЫ АТТЕСТАЦИИ

Дифференцированный зачет- 3 семестр

Адреса электронной версии программы _____

Ростов-на-Дону

2021

Лист согласования

Рабочая программа учебной дисциплины «Информационная безопасность» разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности (специальностям) среднего профессионального образования (далее - СПО) 09.02.05 Прикладная информатика (по отраслям)

Разработчик(и):

Преподаватель _____ С.Н. Маловечко

«30» июня 2021 г.

Рабочая программа рассмотрена и одобрена на заседании предметной (цикловой) комиссии специальностей 09.02.04 Информационные системы (по отраслям) и 09.02.05 Прикладная информатика (по отраслям)

Протокол № «8» от 30 июня 2021 г

Председатель предметной (цикловой) комиссии _____ С.В. Шинакова
30 июня 2021г.

Рецензенты:

_колледж ЭУП ДГТУ_____	__преподаватель__	___Л.А. Белас_____
(место работы)	(занимаемая должность)	(инициалы, фамилия)

СОГЛАСОВАНО:

Заместитель директора по УВР _____ Т.Е. Шепелева

«30» 06 2021 г.

СОДЕРЖАНИЕ

1. ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ 4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 5
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ 9
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ 10

1. ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Область применения программы

Рабочая программа учебной дисциплины «Информационная безопасность» является вариативной частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.04 Информационные системы (по отраслям).

1.2 Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина входит в вариативную часть профессионального цикла как общепрофессиональная дисциплина.

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

Целью освоения дисциплины "Информационная безопасность " является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

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

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности 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.
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности.

Изучение программного материала должно способствовать формированию у студента прочных знаний, устойчивых умений, твердых навыков в области информационной безопасности объектов информатизации.

Коды формируемых компетенций ОК1; ОК2; ОК3; ОК4; ОК5; ОК6; ОК7; ОК8; ОК9.

1.4 Количество часов на освоение программы дисциплины

- максимальной учебной нагрузки обучающегося 72часа в том числе:
- обязательной аудиторной учебной нагрузки обучающегося 48 часов;
- самостоятельной работы обучающегося 18 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)	48
в том числе:	
практические занятия	32
курсовая работа (проект)	
Самостоятельная работа обучающегося (всего)	18
Консультации	6
Итоговая аттестация в форме Дифференцированный зачет	

2.2 Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Анализ информационной безопасности объекта информатизации			
Введение	**Содержание:** Цели и задачи дисциплины информационная безопасность. Роль и место информационной безопасности в современном обществе.	2	1
Тема 1.1. Правовые основы информационной безопасности общества	**Содержание:** Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Закон РФ "Об информации, информатизации и защите информации". Ответственность за нарушения в сфере информационной безопасности. Классификация тайн и их правовое регулирование.	2	2
	Практическое занятие №1 Документы, регламентирующие деятельность в сфере информационной безопасности	2	2
Тема 1.2. Составляющие информационной безопасности	**Содержание:** Основные понятия информационной безопасности. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность**.**	2	1
	Практическое занятие №2 Шифрование информации с применением различных шифров.	2	2
Тема 1.3. Угрозы информационной безопасности в компьютерных системах	**Содержание**: Компьютерная система как объект защиты информации. Понятие угрозы информационной безопасности в компьютерных системах. Классификация и общий анализ угроз информационной безопасности в компьютерных системах. Модель злоумышленника.	2	2
	Практическое занятие №3. Установка ОС Windows 10 на виртуальную машину VirtualBox	2	2
	Практическое занятие №4. Настройка локальной политики безопасности ОС Windows 10	2	2
	Практическое занятие №5. Настройка ограничений использования программ ОС Windows 10	2	2

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	**2**	**3**	4
	Практическое занятие №6. Настройка прав пользователя ОС Windows 10	2	2
	Практическое занятие №7. Настройка брандмаура в ОС Windows 10	2	2
	Практическое занятие №8. Настройка шаблона безопасности в консоле MMC ОС Windows 10	2	2
	Практическое занятие №9. Настройка шаблона безопасности в консоле MMC ОС Windows 10	2	2
	Практическое занятие №10. Настройка аудита системы в ОС Windows 10	2	2
Самостоятельная работа.	Подготовка сообщение на заданную тему	6	1
Консультация по первому разделу		2	
Раздел 2. Криптографические методы и средства защиты информации			
Тема 2.1. Симметричные и ассиметричные криптосистемы.	**Содержание:** Идентификация объекта. Проверка аутентификации. Симметричные системы шифрования. Асимметричные системы шифрования.	2	2
	Практическое занятие №11 Алгоритм шифрования RSA. Вычисление пары ключей шифра RSA	2	2
	Практическое занятие №12. Настройка защиты информации в MS Word 2016	2	2
	Практическое занятие №13. Настройка защиты информации в MS Excel 2016.	2	2
Тема 2.2 Электронно-цифровая подпись	**Содержание:** Цифровая подпись как средство защиты целостности данных. Схема установки ЭЦП. Схема проверки ЭЦП. Роль удостоверяющих центров.	2	2
	Практическое занятие №14 Применение хеш-функции в создании электронной цифровой подписи	2	2
Самостоятельная работа.	Подготовка сообщение на заданную тему	6	1
Консультация по второму разделу		2	

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	**2**	**3**	4
Раздел 3. Информационная безопасность компьютерных сетей			
Тема 3.1 Технологии защиты компьютерных сетей	**Содержание:** Встроенные средства защиты операционных систем. Методы блокирования доступа к операционной системе. Настройка параметров безопасности браузера	2	2
	Практическое занятие № 15. Установка и настройка антивирусных программ.	2	2
Тема 3.2 Межсетевое экранирование	**Содержание:** Системы обнаружения вторжений (Intrusion Detection Systems - IDS), Открытые ключи (Public Key Infrastructure - PKI), виртуальные частные сети (Virtual Private Networks - VPN). Межсетевые экраны (firewalls), Технология межсетевого экранирования, архитектура построения, схемы классификации, функциональные возможности и уязвимости межсетевых экранов.	2	2
	Практическое занятие №16. Настройка параметров безопасности браузера	2	1
Самостоятельная работа.	Подготовка сообщение на заданную тему	6	1
Консультация по третьему разделу		2	
Итого		72	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие учебных кабинетов алгоритмизации и программирования.

Кабинет алгоритмизации и программирования

Оборудование учебного кабинета и рабочих мест кабинета:

- посадочные места по количеству студентов;
- рабочее место преподавателя;
- учебная доска;
- комплект учебно-методической документации;
- сборники задач, тестовых заданий.

Технические средства обучения:

- компьютер;
- мультимедийный проектор.

Лицензионное программное обеспечение: MS Windows 10, Ubuntu 21.04 , MS Office 2016 Professional, VirtualBox

3.2 Информационное обеспечение обучения

Основные источники:

1. С. А Нестеров. Информационная безопасность : учебник и практикум для СПО / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Профессио нальное образование)
2. Т.Л. Партыка, И.И. Попов. Информационная безопасность: учеб. пособие /— 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с.

Дополнительные источники:

1. Мельников В.П., Куприянов А.И. Информационная безопасность, Москва : КноРус, 2018.
2. Валерий Бондарев. Введение в информационную безопасность автоматизированных систем. Учебное пособие. МГТУ им. Н. Э. Баумана, 2016 г.
3. Елена Баранова, Д. Ларин. Информационная безопасность. История защиты информации в России. КДУ, 2016 г.

Интернет-ресурсы:

1. Журнал Информационная безопасность. URL: http://www.itsec.ru/main.php
2. Лаборатория виртуальной учебной литературы. URL: http:// www.gaudeamus.omskcity.com.
3. Информационно-аналитический сайт по ИБ. URL: http://www.anti-malware.ru/
4. Открытая библиотека документов по ИБ . URL: www.SecurityPolicy.RU
5. Защита информации, управление информационной безопасностью и рисками. URL: http://www.iso27000.ru/
6. Энциклопедия. URL: http://www.km.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляются преподавателем в процессе проведения практических занятий, тестирования, а также выполнения студентами индивидуальных заданий.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
1	**2**
Умения:	
классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	оценка результатов выполнения практической работы; устный опрос;
применять основные правила и документы системы сертификации Российской Федерации	оценка результатов выполнения практической работы; устный опрос;
классифицировать основные угрозы безопасности информации	оценка результатов выполнения практической работы; устный опрос;
Знания:	
сущность и понятие информационной безопасности, характеристику ее составляющих	проверка опорных конспектов; проверка докладов; тестирование; устный опрос.
место информационной безопасности в системе национальной безопасности страны	проверка опорных конспектов; проверка докладов; тестирование; устный опрос.
источники угроз информационной безопасности и меры по их предотвращению	интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы; оценка результатов выполнения практической работы.