

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Тарасенко Лидия Александровна
Должность: Директор
Дата подписания: 17.10.2023 12:17:51
Уникальный программный идентификатор:
974f72a491e038b845779dd763f1d39f2c9a325f

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖИ
РЕСПУБЛИКИ КРЫМ
АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ»
«ФИНАНСОВО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ»**

Рассмотрено и одобрено
на заседании педагогического совета
Протокол № 15
От « 31 » 08 2021 г.

УТВЕРЖДАЮ
Директор АНО «ПОО» «ФЭК»
 Л.А. Тарасенко



**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

По специальности:
09.02.04 «Информационные системы (по отраслям)»

Симферополь
2021г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 09.02.04 Информационные системы, Приказ Министерства образования и науки РФ от 14 мая 2014 г. N 525 "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.04 Информационные системы (по отраслям)" (с изменениями и дополнениями)

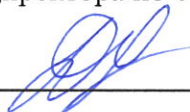
Организация-разработчик: Автономная некоммерческая организация «Профессиональная образовательная организация» «Финансово-экономический колледж».

Разработчик

ГРИБЕЛЬНАЯ Виктория Викторовна – преподаватель АНО «ПОО» «ФЭК»

СОГЛАСОВАНО

Зам. директора по УМР



Н.Ю. Данченко

СОДЕРЖАНИЕ

	СТР.
1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРА УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	6
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	17
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕ ДИСЦИПЛИНЫ	19

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.04 Информационные системы, утвержденного приказом Министерства образования и науки Российской Федерации от 14 мая 2014 г. N 525

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы

В структуре основной профессиональной образовательной программы учебная дисциплина «ОП.13 Информационная безопасность» входит в общепрофессиональный цикл.

1.3. Цель и задачи дисциплины – требования к результатам освоения дисциплины

Требования к результатам освоения дисциплины:

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

осуществлять математическую и информационную постановку задач по обработке информации, использовать алгоритмы обработки информации для различных приложений;

– уметь решать прикладные вопросы интеллектуальных систем с использованием статических экспертных систем, экспертных систем реального времени; использовать языки структурного, объектно-ориентированного программирования и языка сценариев для создания независимых программ, разрабатывать графический интерфейс приложения;

создавать проект по разработке приложения и формулировать его задачи, выполнять управление проектом с использованием инструментальных средств;

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

основные виды и процедуры обработки информации, модели и методы решения задач обработки информации (генерация отчетов, поддержка принятия решений, анализ данных, искусственный интеллект, обработка изображений);

сервисно ориентированные архитектуры, CRM- системы, ERP-системы;

объектно-ориентированное программирование;

спецификации языка, создание графического пользовательского интерфейса (GUI), файловый ввод- вывод, создание сетевого сервера и сетевого клиента;

платформы для создания, исполнения и управления информационной системой;

основные процессы управления проектом разработки

В результате освоения дисциплины обучающийся должен **иметь практический опыт**:

использования инструментальных средств обработки информации;

участия в разработке технического задания;

формирования отчетной документации по результатам работ;
использования стандартов при оформлении программной документации;
программирования в соответствии с требованиями технического задания;
использования критериев оценки качества и надежности функционирования
информационной системы;
применения методики тестирования разрабатываемых приложений;
управления процессом разработки приложений с использованием инструментальных
средств;

В процессе освоения дисциплины у студентов должны формироваться компетенции

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.

ОК 4. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.

ОК 6. Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Быть готовым к смене технологий в профессиональной деятельности.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	144
Обязательная аудиторная учебная нагрузка (всего)	88
в том числе:	
лекционные занятия	12
практические занятия	76
<i>семинарские занятия</i>	
<i>Самостоятельная работа¹</i>	56
Промежуточная аттестация в форме зачета	2

¹Самостоятельная работа в рамках образовательной программы планируется образовательной организацией в соответствии с требованиями ФГОС СПО в пределах объема учебной дисциплины в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

2.2. Тематический план и содержание учебной дисциплины «ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа	Объем часов	Коды компетенций, формированию которых способствует элемент программы
Введение	Введение. Цели, задачи и структура дисциплины. Основные понятия и термины.	2	ОК 01, 02,03,04,05,06,07,08,09
Раздел 1. Борьба с угрозами несанкционированного доступа к информации			
Тема 1.1. Актуальность проблемы обеспечения безопасности информации	<p>Содержание учебного материала Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Возможные угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Виды угроз. Определение требований к уровню обеспечения информационной безопасности.</p>	4	ОК 01, 02,03,04,05,06,07,08,09
	<p>Самостоятельная работа Виды угроз. Определение требований к уровню обеспечения информационной безопасности.</p>	4	ОК 01, 02,03,04,05,06,07,08,09
Тема 1.2. Виды мер обеспечения информационной безопасности	<p>Содержание учебного материала Виды мер обеспечения информационной безопасности: правовые, организационные, технические, программно-математические.</p>	10	ОК 01, 02,03,04,05,06,07,08,09

	<p>Специфические приемы управления техническими средствами. Административный уровень защиты информации: программа безопасности, политика безопасности. Самостоятельная работа Приемы управления техническими средствами защиты информации</p>		
Раздел 2. Защита информации в персональном компьютере			
<p>Тема 2.1. Особенности защиты информации в персональном компьютере</p>	<p>Основные защитные механизмы: идентификация и аутентификация, протоколирование и аудит. Разграничение доступа. Контроль целостности. Обнаружение и противодействие атакам. Защита от копирования информации</p>	14	ОК 01, 02,03,04,05, 06,07,08,09
<p>Тема 2.2. Программные средства защиты информации</p>	<p style="text-align: center;">Практические занятия</p> <p>Изучение программных средств защиты от несанкционированного доступа. Средства безопасности Windows. Обеспечение безопасности хранения данных в ОС Windows. Средства безопасности ASP_NET. Аутентификация. Защита баз данных.</p>	10	
	<p style="text-align: center;">Самостоятельная работа Биометрическая аутентификация</p>	6	
Раздел 3. Криптографические методы защиты информации			
<p>Тема 3.1. Криптология и</p>	<p style="text-align: center;">Содержание учебного материала</p> <p>Основные понятия: криптология, криптография, ключ, криптографическая</p>	4	

основные этапы ее развития	система. Требования к криптографическим методам преобразования информации. Этапы развития криптологии как науки.		
	Самостоятельная работа Требования к криптографическим методам преобразования информации.	10	
Тема 3.2. Методы криптографических преобразований	Содержание учебного материала Классификация криптосистем. Алгоритмы шифрования. Шифры замены. Шифры перестановки. Ассиметричное шифрование: метод гаммирования и аналитического преобразования данных	10	
	Практические занятия Разработка простейших криптографических алгоритмов на основе методов замены. Разработка простейших криптографических алгоритмов на основе методов перестановки.	8	
	Самостоятельная работа. Криптографические методы защиты информации.	6	
Тема 3.3. Стандарты шифрования	Содержание учебного материала История создания стандартов шифрования DES и RSA. Алгоритм шифрования с использованием симметричного стандарта DES. Алгоритм шифрования с использованием симметричного стандарта RSA.	6	

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа	Объем часов	Уровень освоения
	Практические занятия Шифрование информации с использованием стандарта DES. Шифрование информации с использованием стандарта RSA.	4	2
	Самостоятельная работа Изучение стандартов шифрования AES и Rjndael	6	3

Раздел 4. Борьба с вирусным заражением информации

<p align="center">Тема 4.1. Проблема вирусного заражения и структура современных вирусов</p>	<p>Содержание учебного материала Компьютерный вирус: понятие, пути распространения, проявление действия вируса. Структура современных вирусов: модели поведения вирусов; деструктивные действия вируса; разрушение программы защиты, схем контроля или изменение состояния программной среды; воздействия на программно-аппаратные средства защиты информации. Программы-шпионы. Взлом парольной защиты. Защита от воздействия вирусов.</p>	4	1
	<p>Самостоятельная работа обучающихся Изучение литературы по теме: Компьютерные вирусы. Структура современных вирусов.</p>	6	3
<p align="center">Тема 4.2. Классификация антивирусных программ</p>	<p>Содержание учебного материала Программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры. Профилактика заражения вирусом. Защита информации в сетях.</p>	4	1
	<p>Практические занятия Антивирусные программы</p>	4	2
	<p>Самостоятельная работа Работа с антивирусными программами</p>	6	3
Раздел 5. Организационно-правовое обеспечение информационной безопасности			
<p align="center">Тема 5.1. Международные, российские и</p>	<p>Содержание учебного материала Опыт законодательного регулирования информатизации в России и за рубежом. Концепция правового обеспечения информационной безопасности Российской</p>	6	1

отраслевые правовые документы	Федерации. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Международные правовые акты по защите информации. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.		
	Самостоятельная работа Международные правовые акты по защите информации.	4	3
	Зачет	2	
	Всего:	144	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

3.1. Материально-техническое обеспечение реализации программы

Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения: учебного кабинета информатики

Оборудование учебного кабинета:

- посадочные места по количеству студентов;
- рабочее место преподавателя, оборудованное персональным компьютером с лицензионным или свободно распространяемым программным обеспечением, соответствующим разделам программы и подключенным к сети Интернет и средствами вывода звуковой информации;
- рабочие места студентов, оборудованные персональным компьютером с лицензионным или свободно распространяемым программным обеспечением, соответствующим разделам программы и подключенным к сети Интернет и средствами вывода звуковой информации;
- комплект методических пособий по практическим работам;
- сканер;
- принтер
- **Учебно-методические средства обучения:**
 - тематические папки дидактических материалов;
 - комплект учебно-методической документации;
 - комплект учебников (учебных пособий) по количеству обучающихся.
- **Технические средства обучения:**
 - мультимедийный проектор;
 - web-камера;
 - фото или/и видеокамера

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

3.2.1. Основные источники

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. - Москва: **Наука**, 2015. - 552 с.
2. Бабаш, А. В. Информационная безопасность (+ CD-ROM) / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Основы информационно-психологической безопасности: моногр. . - М.: Международный гуманитарный фонд "Знание", 2014. - 416 с.
4. Безопасность ребенка. Информационный стенд. - М.: Сфера, Ранок, 2013. - 787 с.
5. Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2015. - 368 с.
6. Гафнер, В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2014. - 336 с.
7. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2015. - 240 с.
8. Девянин, П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П.Н. Девянин. - М.: Радио и связь, 2013. - 176 с.
9. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт / Л.Л. Ефимова, А.С. А, Кочерга. - М.: Юнити-Дана, 2013. - 240 с.
10. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. - Москва: **Машиностроение**, 2016. - 536 с.
11. Информационная безопасность открытых систем. В 2 томах. Том 2. Средства защиты в сетях / С.В. Запечников и др. - Москва: **СПб. [и др.] : Питер**, 2014. - 560 с.
12. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2017. - 336 с.
13. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Академия, 2013. - 336 с.
14. Мельников, В. П. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - Москва: **Мир**, 2013. - 336 с.
15. Мельников, В.П. Информационная безопасность и защита информации / В.П. Мельников. - М.: Академия (Academia), 2016. - 282 с.
16. Партыка, Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2016. - 368 с.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.12 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Результаты обучения	Критерии оценки	Формы и методы оценки
<p><i>Перечень знаний, осваиваемых в рамках дисциплины:</i></p> <p>методы хранения чисел в памяти электронно-вычислительной машины (далее – ЭВМ) и действия над ними, оценку точности вычислений;</p> <p>методы решения основных математических задач – интегрирования, дифференцирования, решения линейных и трансцендентных уравнений и систем уравнений с помощью ЭВМ.</p>	<p>«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.</p> <p>«Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.</p> <p>«Удовлетворительно» -</p>	<p>Примеры форм и методов контроля и оценки</p> <ul style="list-style-type: none"> •Компьютерное тестирование на знание терминологии по теме •Тестирование •Контрольная работа •Самостоятельная работа •Защита реферата •Семинар •Защита курсовой работы (проекта) •Выполнение проекта
<p><i>Перечень умений, осваиваемых в рамках дисциплины:</i></p> <p>использовать основные численные методы решения математических задач;</p> <p>выбирать оптимальный численный метод для решения поставленной задачи;</p> <p>давать математические характеристики точности исходной информации и оценивать точность полученного численного решения;</p> <p>разрабатывать алгоритмы и программы для решения вычислительных задач, учитывая необходимую точность получаемого результата.</p>	<p>теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки.</p> <p>«Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.</p>	<ul style="list-style-type: none"> •Наблюдение за выполнением практического задания. (деятельностью студента) •Оценка выполнения практического задания(работы) •Подготовка и выступление с докладом, сообщением, презентацией •Решение ситуационной задачи

