Министерство образования и науки Челябинской области
Автономная некоммерческая организация
профессионального образования
«Челябинский колледж Комитент»
(АНОПО «Челябинский колледж Комитент»)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность: 09.02.07 Информационные системы и программирование

Квалификация выпускника: администратор баз данных
на базе среднего общего образования

Челябинск 2025

Содержание

1. Общая характеристика рабочей программы дисциплины ОП.13 Информационная безопасность

1.1. Место дисциплины в структуре образовательной программы:

Дисциплина ОП.13 Информационная безопасность: является обязательной частью профессионального цикла образовательной программы по специальности 09.02.07 Информационные системы и программирование

1.2. Цель и планируемые результаты освоения дисциплины:

В результате освоения дисциплины ОП.13 Информационная безопасность:

уметь:

- применять технические, программные, организационные, правовые и криптографические методы и средства защиты информации.

знать:

- источники возникновения информационных угроз;
- модели и принципы защиты информации от несанкционированного доступа;
- методы защиты информации в информационных базах данных;
- методы антивирусной защиты информации;
- концепцию правового обеспечения информационной безопасности.

Перечень формируемых компетенций

Общие компетенции (ОК):

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 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 09. Использовать информационные технологии в профессиональной деятельности.

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

Профессиональные компетенции (ПК)

ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев

ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей

ПК 3.3. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации

Личностные результаты:

Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации	**ЛР 16**
Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм	**ЛР 17**
Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.	**ЛР 18**
Формировать алгоритмы разработки программных модулей в соответствии с техническим заданием.	**ЛР 22**
Разрабатывать техническое задание на сопровождение информационной системы, дизайн-концепции веб-приложений в соответствии с корпоративным стилем заказчика, требования к программным модулям на	**ЛР 23**

основе анализа проектной и технической документации на предмет взаимодействия компонент.	
Выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов.	**ЛР 24**
Активно применять полученные знания на практике	**ЛР 25**

2 Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Объем образовательной программы дисциплины	**76**
в том числе в форме практической подготовки	*10*
в том числе:	
теоретическое обучение	**48**
практические занятия	**28**
консультации	
самостоятельная работа	
Промежуточная аттестация в форме	Дифференцированный зачет

2.2. Тематический план и содержание дисциплины ОП.13 Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Осваиваемые элементы компетенций и личностные результаты
1	2	3	4
	2 семестр		
Тема 1. Введение.	**Содержание учебного материала**	**14**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1., ПК 3.1., ПК 3.3. ЛР 16-18, 22-25
	Введение. Основные понятия и определения. Взаимосвязь с другими дисциплинами	8	
	Практические занятия	6	
	Практическая работа №1.Виды и назначение различных мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Специфические приемы управления техническими средствами с целью пресечения несанкционированного доступа. Практическая работа№2.Разграничение доступа к системам Практическая работа№3.Защита информации от копирования: задание не копируемых меток Практическая работа№4.Защита программ в оперативной памяти Практическая работа№5.Защита программ от дисассемблирования.. Практическая работа№6.Приемы работы с защищенными программами		
Тема 2. Основные понятия и определения.	**Содержание учебного материала**	**14**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1., ПК 3.1., ПК 3.3. ЛР 16-18, 22-25
	Актуальность защиты информационных ресурсов в компьютерных системах. Основные понятия об информационной безопасности в компьютерных системах. Основные преднамеренные и непреднамеренные угрозы информационной безопасности. Задачи обеспечения безопасности информации в компьютерных системах. Уровни системы защиты информации. Концепция создания защищенных компьютерных систем. Этапы создания комплексной системы защиты информации. Стандарты защищенности компьютерных систем.	8	
	Практическая работа	6	
	Практическая работа№7.Приёмы работы с защищенными программами Практическая работа№8.Перехват вывода на экран Практическая работа№9.Перехват ввода с клавиатуры. Практическая работа№10.Перехват и обработка файловых операций. Практическая работа№11.Пакеты антивирусных программ Практическая работа№12.Брандмауэры и файерволы		
Тема 3. Методы защиты программно-	**Содержание учебного материала**	**12**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1., ПК 3.1., ПК 3.3.
	Архитектура электронных систем обработки данных. Пользовательский, прикладной и программный интерфейсы. Ресурсы компьютера. Вычислительные сети и их ресурсы.	8	

аппаратными средствами КС	Функционирование ЛВС с архитектурой "клиент-сервер". Понятие методов и средств защиты. Схема классификации методов и средств комплексной защиты ИПО. Защита информации от хищения. Защита информации от потери. Защита программ от сбоев и отказов.		ЛР 16-18, 22-25
	Практические занятия	4	
	Практическая работа№12. Организация резервного копирования средствами ОС. Практическая работа№13. Методов и средств защиты Практическая работа№14.Защита от сбоев. Методы применения. Назначения.		
Тема 4. Защита информации в КС от несанкционированного доступа	**Содержание учебного материала**	**12**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1., ПК 3.1., ПК 3.3. ЛР 16-18, 22-25
	Цели, функции и методы защиты ИПО ВС. Общие требования к защищенности КС от несанкционированного изменения структур. Управление доступом процессов к информационным ресурсам. Матричное управление. Мандатное управление. Система разграничения доступом. Концепция построения систем разграничения доступом	8	
	Практические занятия	4	
	Практическая работа №15. Управление правами доступа к файловой системе на базе ОС Windows 2003 Server Практическая работа №16. Управление правами доступа к файловой системе на базе ОС Linux Практическая работа №17. Управление пользовательскими привилегиями с помощью объектов групповых политик (GPO) в домене на базе ОС Windows 2003 Server		
Тема 5. Криптографические методы защиты информации в компьютерных системах	**Содержание учебного материала**	**12**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1., ПК 3.1., ПК 3.3. ЛР 16-18, 22-25
	Шифрование. Основные понятия. Требования к современным методам шифрования. Метод прямой замены. Шифр Вижинера. Метод перестановки. Маршрут Гамильтона. Поточные шифры, блочные шифры. Методы генерации криптографические качественных псевдослучайных последовательностей. Асимметричные системы шифрования (системы с открытым ключом). Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости. Отечественный стандарт шифрования данных ГОСТ 28147-89: алгоритм, скорость работы на различных платформах, режимы пользования.	8	
	Практические занятия	4	
	Практическая работа№18 Разработка программного комплекса «Шифрование информации с помощью методов замены и перестановки». Практическая работа №19: Проверочный тест «Криптографические методы защиты» Практическая работа№20: Работа с перестановочным ключом, использование методов защиты. информации		
Тема 6. Защита компьютерных систем от удаленных атак	**Содержание учебного материала**	**12**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1., ПК 3.1., ПК 3.3.
	Состав и назначение основных компонентов распределенных компьютерных систем. Обеспечение безопасности информации в коммуникационной подсистеме. Основные схемы	8	

	сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации защищенных корпоративных сетей. Понятия аутентификации, авторизации, аудита. Алгоритмы аутентификации. Сетевая аутентификация на основе многоразового пароля. Аутентификация с использованием одноразового пароля.		ЛР 16-18, 22-25
	Практические занятия	4	
	Практическая работа №21. Защита текстовых редакторов в программах WORD Практическая работа №22. Защита электронных таблиц в программах Excel		
Промежуточная аттестация	Дифференцированный зачет		ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10, ПК 2.1., ПК 3.1., ПК 3.3. ЛР 16-18, 22-25
Всего:		**76**	

3. Условия реализации дисциплины

3.1. Требования к материально-техническому обеспечению

Для реализации программы дисциплины должно быть предусмотрено следующее специальное помещение**: Лаборатория программного обеспечения и сопровождения компьютерных систем.** Помещение лаборатория должно соответствовать требованиям Санитарно-эпидемиологических правил и нормативов оснащено типовым оборудованием, в том числе специализированной учебной мебелью и средствами обучения, необходимыми для выполнения требований к уровню подготовки обучающихся.

Лаборатория программного обеспечения и сопровождения компьютерных систем.

Оборудование лаборатории:

Парты (2-х местная)
Стулья
Стол преподавателя
Стул преподавателя
Компьютер
Доска меловая

Лаборатория программного обеспечения и сопровождения компьютерных систем обеспечена необходимым комплектом лицензионного программного обеспечения

Библиотека, читальный зал с выходом в Интернет

Материальное оснащение, компьютерное и интерактивное оборудование:

Автоматизированное рабочее место библиотекаря
Автоматизированное рабочее место читателей
Автоматизированное рабочее место для лиц с ОВЗ
Принтер
Сканер
Стеллажи для книг
Кафедра
Выставочный стеллаж
Каталожный шкафа
Посадочные места (столы и стулья для самостоятельной работы)

Помещение для самостоятельной работы

Материальное оснащение, компьютерное и интерактивное оборудование:

Автоматизированные рабочие места обучающихся
Парты (2-х местные)
Стулья

Автоматизированные рабочие места обеспечены доступом в электронную информационно-образовательную среду АНОПО «Челябинский колледж Комитент», с выходом в информационно-коммуникационную сеть «Интернет».

3.2. Информационное обеспечение реализации программы

Основная литература:

1.Нестеров, С. А. Информационная безопасность : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Профессиональное образование). — ISBN 978-5-534-07979-1.

Дополнительная литература:

1. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.

4. Контроль и оценка результатов освоения дисциплины

Результаты обучения	Критерии оценки	Методы оценки
уметь: -применять технические, программные,	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать	Проверка практических работ, конспектов. Дифференцированн

организационные, правовые и криптографические методы и средства защиты информации. ***знать:*** - источники возникновения информационных угроз; - модели и принципы защиты информации от несанкционированного доступа; - методы защиты информации в информационных базах данных; - методы антивирусной защиты информации; - концепцию правового обеспечения информационной безопасности.	теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними дискуссионными навыками и приемами, активно проявляет себя в групповой работе; Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении дискуссионных вопросов и задач, владеет необходимыми навыками и приемами их выполнения, способен проявлять себя в групповой работе; Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач, не активен в групповой работе; Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно, не принимает участие в групповой работе.	ый зачет.