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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ОП.11 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Специальность: 09.02.03 Программирование в компьютерных системах

Квалификация выпускника: Техник - программист

Челябинск 2020

Содержание

1.Общая характеристика рабочей программы дисциплины ОП.11 Информационная безопасность

1.1. Место дисциплины в структуре образовательной программы:

Дисциплина ОП.11 Информационная безопасность: является вариативной частью общепрофессионального учебного цикла образовательной программы по специальности 09.02.03 Программирование в компьютерных системах базовой подготовки.

1.2. Цель и планируемые результаты освоения дисциплины:

В результате освоения дисциплины ОП.11 Информационная безопасность:

уметь:

- классифицировать возможные угрозы безопасности компьютерной системе;
- выбирать и применять методы защиты компьютерной информации при проектировании компьютерных систем.

знать:

- правовые основы защиты компьютерной информации;
- организационные, технические и программные методы защиты информации в компьютерной системе;
- модели и методы шифрования;
- методы идентификации пользователей;
- методы защиты программ от программных закладок и вирусов

Перечень формируемых компетенций

Общие компетенции (ОК):

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

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

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

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

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

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

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Профессиональные компетенции (ПК)

ПК 1.1. Выполнять разработку спецификаций отдельных компонент.

ПК 1.2. Осуществлять разработку кода программного продукта на основе готовых спецификаций на уровне модуля.

ПК 1.3. Выполнять отладку программных модулей с использованием специализированных программных средств.

ПК 1.4. Выполнять тестирование программных модулей.

ПК 1.5. Осуществлять оптимизацию программного кода модуля.

ПК 1.6. Разрабатывать компоненты проектной и технической документации с использованием графических языков спецификаций.

ПК 2.1. Разрабатывать объекты базы данных.

ПК 2.2. Реализовывать базу данных в конкретной системе управления базами данных.

ПК 2.3. Решать вопросы администрирования базы данных.
ПК 2.4. Реализовывать методы и технологии защиты информации в базах данных.
ПК 3.1. Анализировать проектную и техническую документацию на уровне взаимодействия компонент программного обеспечения.
ПК 3.2. Выполнять интеграцию модулей в программную систему.
ПК 3.3. Выполнять отладку программного продукта с использованием специализированных программных средств.
ПК 3.4. Осуществлять разработку тестовых наборов и тестовых сценариев.
ПК 3.5. Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.
ПК 3.6. Разрабатывать технологическую документацию

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	**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 основе анализа проектной и технической документации на предмет взаимодействия компонент.	**ЛР 23**
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	5 семестр	6 семестр	7 семестр	8 семестр
Объем образовательной программы дисциплины	**233**	**39**	**40**	**78**	**76**
в том числе в форме практической подготовки	-	-	*2*	*4*	*4*
в том числе:					
теоретическое обучение	**111**	16	18	40	37
практические занятия	**49**	10	10	12	17
консультации					
самостоятельная работа	**73**	13	12	26	22
Промежуточная аттестация в форме			Зачет		Экзамен

2.2. Тематический план и содержание дисциплины ОП.11 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
	5 семестр		
Тема 1. Введение.	**Содержание учебного материала**	**15**	ОК 1. - ОК 9. ПК 1.1-ПК 1.6 ПК 2.1-ПК 2.4 ПК 3.1-ПК 3.6 ЛР 16-18, 22-25
	Введение. Основные понятия и определения. Взаимосвязь с другими дисциплинами	4	
	Практическая работа	5	
	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		
	Самостоятельная работа обучающихся	6	
	1.Использование технической документации ПК 2.Средства защиты и отладки ПО 3.Методы защиты от копирования		
Тема 2. Основные понятия и определения.	**Содержание учебного материала**	**24**	ОК 1. - ОК 9. ПК 1.1-ПК 1.6 ПК 2.1-ПК 2.4 ПК 3.1-ПК 3.6 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.	12	
	Практическая работа	5	

	Работа №1.Приёмы работы с защищенными программами Работа№2.Перехват вывода на экран Работа№3.Перехват ввода с клавиатуры. Работа№4.Перехват и обработка файловых операций. Работа№5.Пакеты антивирусных программ Работа№6.Брандмауэры и файерволы		
	Самостоятельная работа учащихся	7	
	1 Использование программных средств защиты информации 2. Установка и тестирование программ для поиска заражённых файлов и приложений		
6 семестр			
Тема 3. Методы защиты программно-аппаратными средствами КС	**Содержание учебного материала**	**40**	ОК 1. - ОК 9. ПК 1.1-ПК 1.6 ПК 2.1-ПК 2.4 ПК 3.1-ПК 3.6 ЛР 16-18, 22-25
	Архитектура электронных систем обработки данных. Пользовательский, прикладной и программный интерфейсы. Ресурсы компьютера. Вычислительные сети и их ресурсы. 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.	18	
	Практическая работа	10	
	Работа №1. Организация резервного копирования средствами ОС. Работа№2. Методов и средств защиты Работа№3.Защита от сбоев. Методы применения. Назначения.		
	Самостоятельная работа учащихся	12	
	Изучения литературы. Конспектирование. Установка и коррекция защиты программ. Подготовка к зачету.		
Промежуточная аттестация	**Зачет**		ОК 1. - ОК 9. ПК 1.1-ПК 1.6 ПК 2.1-ПК 2.4 ПК 3.1-ПК 3.6 ЛР 16-18, 22-25
7 семестр			
Тема 4. Защита информации в КС от несанкционированного доступа	**Содержание учебного материала**	**78**	ОК 1. - ОК 9. ПК 1.1-ПК 1.6 ПК 2.1-ПК 2.4 ПК 3.1-ПК 3.6 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	40	

	Практическая работа	12	
	Практическая работа № 1. Управление правами доступа к файловой системе на базе ОС Windows 2003 Server Практическая работа № 2. Управление правами доступа к файловой системе на базе ОС Linux Практическая работа № 3. Управление пользовательскими привилегиями с помощью объектов групповых политик (GPO) в домене на базе ОС Windows 2003 Server		
	Самостоятельная работа учащихся.	26	
	Реферат на тему: «Модели защиты при отказе в обслуживании», «Модели безопасности по разграничению доступа в систему», «Модель безопасности объектов ВС», Классификация компьютерных вирусов», «Политики безопасности», Виды антивирусных программ» Составление конспектов по теме: Защита информации в КС от несанкционированного доступа. Методы. Способы защиты. Подготовка к практической работе. Контрольной работе.		
8 семестр			
Тема 5. Криптографические методы защиты информации в компьютерных системах	**Содержание учебного материала**	**40**	ОК 1. - ОК 9. ПК 1.1-ПК 1.6 ПК 2.1-ПК 2.4 ПК 3.1-ПК 3.6 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.	20	
	Практическая работа	10	
	Работа№1 Разработка программного комплекса «Шифрование информации с помощью методов замены и перестановки». Работа №2: Проверочный тест «Криптографические методы защиты» Работа№3: Работа с перестановочным ключом, использование методов защиты. информации		
	Самостоятельная работа учащихся.	10	
	Подготовка к практическим работам. Изучение конспектов. Составление сводных таблиц по теме: «Криптографические методы защиты»		
Тема 6. Защита компьютерных систем от удаленных атак	**Содержание учебного материала**	**36**	ОК 1. - ОК 9. ПК 1.1-ПК 1.6 ПК 2.1-ПК 2.4 ПК 3.1-ПК 3.6 ЛР 16-18, 22-25
	Состав и назначение основных компонентов распределенных компьютерных систем. Обеспечение безопасности информации в коммуникационной подсистеме. Основные схемы 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	17	

	одноразового пароля.		
	Практическая работа	7	
	Работа№1. Защита текстовых редакторов в программах WORD Работа№2. Защита электронных таблиц в программах Excel		
	Самостоятельная работа учащихся.	12	
	Подготовка к практическим работам. Изучение способов защиты КС. Подготовка к экзамену.		
Промежуточная аттестация	Экзамен		ОК 1. - ОК 9. ЛР 16-18, 22-25
Всего:		**233**	

3. Условия реализации дисциплины

3.1. Требования к материально-техническому обеспечению

Для реализации программы дисциплины должно быть предусмотрено следующее специальное помещение**: Лаборатория информационно-коммуникационных систем.** Помещение кабинета должно соответствовать требованиям Санитарно-эпидемиологических правил и нормативов (СанПиН 2.4.2 № 178–02): оснащено типовым оборудованием, в том числе специализированной учебной мебелью и средствами обучения, необходимыми для выполнения требований к уровню подготовки обучающихся.

Лаборатория информационно-коммуникационных систем.

Оборудование учебного кабинета:

Парты (2-х местная)
Стулья
Стол преподавателя
Стул преподавателя
Компьютеры
Доска меловая
Лаборатория информационно-коммуникационных 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.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.
2. 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.
3. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с..

4. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 с.
5. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с

4. Контроль и оценка результатов освоения дисциплины

Результаты обучения	Критерии оценки	Методы оценки
уметь: - классифицировать возможные угрозы безопасности компьютерной системе; - выбирать и применять методы защиты компьютерной информации при проектировании компьютерных систем. ***знать:*** - правовые основы защиты компьютерной информации; - организационные, технические и программные методы защиты информации в компьютерной системе; - модели и методы шифрования; - методы идентификации пользователей; методы защиты программ от программных закладок и вирусов	Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал курса, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать 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.	Проверка практических работ, конспектов. Анализ работы самостоятельной работы учащегося. Заслушивание рефератов. Контрольная работа. Зачет. Экзамен.