

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Романчук Иван Сергеевич  
Должность: Ректор  
Дата подписания: 19.06.2024 17:51:18  
Уникальный программный ключ:  
e68634da050325a9234284dd96b4f0f8b288e139

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФГАОУ ВО «Тюменский государственный университет»  
Тобольский педагогический институт им. Д.И.Менделеева (филиал)  
Тюменского государственного университета



УТВЕРЖДАЮ  
Заместитель директора филиала  
*Шитиков П.М.*  
Шитиков П.М.  
«02» 02 2023 год

**ОП.14 Методы и средства защиты компьютерной информации**  
Рабочая программа дисциплины для обучающихся  
по программе подготовки специалистов среднего звена  
09.02.07 Информационные системы и программирование  
форма обучения очная

Оленькова Маргарита Николаевна Методы и средства защиты компьютерной информации. Рабочая программа дисциплины для обучающихся по программе подготовки специалистов среднего звена 09.02.07 Информационные системы и программирование. Форма обучения – очная. Тобольск, 2022.

Рабочая программа дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденный приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 года, № 1547.

Рабочая программа дисциплины опубликована на сайте ТюмГУ: Методы и средства защиты компьютерной информации. [электронный ресурс] / Режим доступа: <https://www.utmn.ru/sveden/education/#>

© Тобольский педагогический институт им. Д.И. Менделеева (филиал) Тюменского государственного университета, 2022

© Оленькова Маргарита Николаевна , 2022

## Содержание

1. Паспорт рабочей программы дисциплины.....	4
2. Структура и содержание учебной дисциплины.....	5
3. Условия реализации программы.....	9
4. Контроль и оценка результатов освоения дисциплины.....	10

## 1. Паспорт рабочей программы дисциплины

### 1.1. Область применения программы

Рабочая программа дисциплины – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

### 1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена:

Дисциплина входит в Общепрофессиональный цикл учебного плана специальности.

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

Код ПК, ОК	Умения	Знания
ОК01 ОК02 ОК04 ОК06 ПК 11.1 ПК 11.2 ПК 11.6	<p>- применять правовые, организационные, технические и программные средства защиты информации;</p> <p>- проводить оценку угроз безопасности объекта информатизации;</p> <p>- реализовывать простые информационные технологии реализующие методы защиты информации.</p>	<p>- применять правовые, организационные, технические и программные средства защиты информации;</p> <p>- проводить оценку угроз безопасности объекта информатизации;</p> <p>- реализовывать простые информационные технологии реализующие методы защиты информации.</p>

Результатом освоения программы учебной дисциплины является овладение обучающимися элементами общих (ОК) и профессиональных (ПК) компетенций, включающими способность:

ОК 01.Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК 02.Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности

ОК 04.Эффективно взаимодействовать и работать в коллективе и команде

ОК 06.Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ПК 11.1. Осуществлять сбор, обработку и анализ информации для проектирования баз данных.

ПК 11.2. Проектировать базу данных на основе анализа предметной области.

ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.

### 1.4. Количество часов на освоение дисциплины:

Семестр(ы) 2;

Максимальной учебной нагрузки обучающегося 68 академических часов, в том числе: обязательной аудиторной нагрузки обучающегося 66 академических часов; самостоятельной работы обучающегося 2 академических часа.

## 2. Структура и содержание учебной дисциплины

### 2.1. Объем учебной дисциплины и виды учебной работы

<b>Вид учебной работы</b>	<b>Объем в ак. часах</b>
<b>Максимальная учебная нагрузка (всего)</b>	<b>68</b>
<b>Обязательная аудиторная учебная нагрузка (всего)</b>	<b>66</b>
в том числе:	
теоретическое обучение	22
лабораторные работы	44
Самостоятельная работа	2
<b>Промежуточная аттестация в виде комплексного дифференцированного зачета во 2 семестре</b>	

## 2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в ак. часах	Уровень освоения
<b>Раздел 1.</b>	<b>Информационная безопасность и уровни ее обеспечения</b>		
<b>Тема 1.1.</b> Понятия и составляющие информационной безопасности	Содержание учебного материала		
	1   Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Модели безопасности. Понятие «национальная безопасность». Доктрина безопасности Российской Федерации	4	1
	2   Понятия информации. Классификация информации по категории доступа. Виды информации. Понятие ценности информации. Перечень сведений, доступ к которым не может быть ограничен. Понятие конфиденциальной информации, ее виды.		
	3   Концепция информационной безопасности.		
	<b>Самостоятельная работа обучающихся:</b> Подготовить реферат на тему: «Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства)», «Угрозы информационной безопасности Российской Федерации»	2	3
<b>Тема 1.2.</b> Угрозы информационной безопасности в компьютерных системах	Содержание учебного материала		
	1   Классы угроз информационной безопасности	4	1
	2   Каналы несанкционированного доступа к информации		
<b>Тема 1.3.</b> Правовые основы информационной безопасности и защита интеллектуальной собственности	Содержание учебного материала		
	1   Нормативно-правовые документы, регламентирующие отношения в сфере информационной безопасности. Предмет и задачи правового обеспечения информационной безопасности. Законодательство о безопасности и защите информации, его структура и содержание.	2	1
	2   Стандарты информационной безопасности в РФ		
	3   Административный, процедурный, программно-технический уровни информационной безопасности		
	<b>Лабораторные работы</b>	6	2
Доктрина информационной безопасности			
<b>Раздел 2.</b>	<b>Компьютерные вирусы и их защита</b>		
<b>Тема 2.1.</b> Вирусы как	Содержание учебного материала	2	1

угроза информационной безопасности. Средства антивирусной защиты.	1	Компьютерные вирусы и информационная безопасность	4	2
	2	Классификация компьютерных вирусов		
	3	Антивирусные программы. Обнаружение неизвестного вируса		
	<b>Лабораторные работы</b>			
Способы защиты от вирусов. Антивирусные программы.				
<b>Раздел 3.</b>	<b>Информационная безопасность вычислительных сетей</b>			
<b>Тема 3.1.- 3.3.</b> Информационная безопасность вычислительных сетей	Содержание учебного материала		4	1
	1	Особенности информационной безопасности в компьютерных сетях		
	2	Классификация удаленных угроз в вычислительных сетях		
	3	Типовые удаленные атаки и их характеристика		
<b>Раздел 4.</b>	<b>Механизмы обеспечения «Информационной безопасности»</b>			
<b>Тема 4.1. - 4.6</b> Защита информации от несанкционированного доступа.	Содержание учебного материала			
	1	Способы несанкционированного доступа к информации в компьютерных системах.	4	1
	2	Характеристика средств защиты информации в компьютерных системах от несанкционированного доступа.		
	3	Идентификация и аутентификация пользователей: основные понятия, парольная аутентификация, виды паролей, биометрическая аутентификация.		
	4	Управление доступом: основные понятия, виды разграничения доступа, особенности дискреционного, мандатного и ролевого управления доступом.		
	<b>Лабораторные работы</b>		14	2,3
	Обеспечения информационной безопасности средствами Windows 7			
	Защита информации на основе механизмов идентификации и аутентификации			
	Защита папок и файлов			
	Протоколирование и аудит: основные понятия, активный аудит.			
Защита программных средств от несанкционированного копирования и исследования.				
<b>Тема 4.7.</b> Криптографические методы защиты информации	Содержание учебного материала		6	1
	1	Криптография и шифрование. Развитие криптографических систем.		
	2	Классификация криптографических средств.		
	3	Симметричные криптосистемы: DES и ее модификации.		

	4	Ассиметричные криптосистемы: однонаправленные функции, RSA, принципы построения.		
	5	Методы шифрования: замены, перестановки, аналитические, аддитивные, комбинированные.		
	6	Функция хэширования.		
	<b>Лабораторные работы</b>			
		Основы криптографической защиты информации.		
		Шифрование информации с использованием стандарта DES		
		Изучение криптосистемы RSA		
		Настройка и использование межсетевого экрана в ОС Windows XP		
		Электронная цифровая подпись и ее применение для контроля целостности программ и данных.	20	2
		Криптографический интерфейс приложений операционной системы Windows (CryptoAPI): принципы построения и особенности применения.		
		Компьютерная стеганография и ее применение.		
		<b>Всего:</b>	<b>68</b>	

Примечание - для характеристики уровня освоения учебного материала используются следующие обозначения:

1. - Ознакомительный (узнавание ранее изученных объектов, свойств);
2. - Репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. - Продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)



### 3. Условия реализации программы

#### 3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы предполагает наличие кабинета информатики

Основное оборудование:

Столы – 10 шт.

Стулья – 20 шт.

Рабочее место преподавателя - 1,

Доска аудиторная -1 шт.

Технические средства обучения:

Персональный компьютер - 1 шт.

Мобильная интерактивная ЖК-панель – 1шт.,

Планшеты – 15 шт.

На ПК установлено следующее программное обеспечение: Офисное ПО: операционная система iOS. Специализированное ПО: Adobe Photoshop Extended CS5 (№ лицензии 7975804 от 15.10.2010), Adobe Design Premium CS4 (№ лицензии 19532640 от 23.07.2009), MathCAD 14.0 (№ лицензии 2522615 от 19.12.2008), ИКАР Notebook, GIMP, Inkscape. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

#### 3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

##### Основная литература:

Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забаурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/497433>

##### Дополнительная литература:

Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189328>

##### Интернет-ресурсы:

1. Знаниум - <https://new.znanium.com/>
2. Лань - <https://e.lanbook.com/>
3. Юрайт - <https://urait.ru/>
4. IPR SMART - <http://www.iprbookshop.ru/>
5. Elibrary - <https://www.elibrary.ru/>
6. Национальная электронная библиотека (НЭБ) - <https://rusneb.ru/>
7. Межвузовская электронная библиотека (МЭБ) - <https://icdlib.nspu.ru/>
8. "ИВИС" (БД периодических изданий) - <https://dlib.eastview.com/browse>
9. Электронная библиотека Тюмгу - <https://library.utmn.ru/>

**Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине:** Платформа для электронного обучения MicrosoftTeams.

#### 4. Контроль и оценка результатов освоения дисциплины

<i>Результаты обучения</i>	<i>Критерии оценки</i>	<i>Формы и методы оценки</i>
<p><i>Перечень умений, осваиваемых в рамках дисциплины:</i></p> <ul style="list-style-type: none"> <li>- применять правовые, организационные, технические и программные средства защиты информации;</li> <li>- проводить оценку угроз безопасности объекта информатизации;</li> <li>- реализовывать простые информационные технологии реализующие методы защиты информации.</li> </ul>	<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</p>	<p>Индивидуальные задания устный опрос Контрольные вопросы Промежуточная аттестация в виде комплексного дифференцированного зачета во 2 семестре</p>
<p><i>Перечень знаний, осваиваемых в рамках дисциплины:</i></p> <ul style="list-style-type: none"> <li>- применять правовые, организационные, технические и программные средства защиты информации;</li> <li>- проводить оценку угроз безопасности объекта информатизации;</li> <li>- реализовывать простые информационные технологии реализующие методы защиты информации.</li> </ul>	<p>недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.</p> <p>«Удовлетворительно» – 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>	