

**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ТЮМЕНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ТЮМЕНСКОЙ ОБЛАСТИ
«ТЮМЕНСКИЙ ТЕХНИКУМ ИНДУСТРИИ ПИТАНИЯ, КОММЕРЦИИ И СЕРВИСА»
МЕЖРЕГИОНАЛЬНЫЙ ЦЕНТР КОМПЕТЕНЦИЙ В ОБЛАСТИ ИСКУССТВА,
ДИЗАЙНА И СФЕРЫ УСЛУГ**

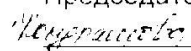
**РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.11 БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ В ЦИФРОВОЙ СРЕДЕ**

Тюмень 2026

Рабочая программа учебной дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 43.02.15 Повар-кондитерское дело

Разработчики: Карпова М.В., преподаватель первой квалификационной категории

Рассмотрено и одобрено
на заседании ПЦК ИПиС
Протокол № 10 от 28.05.2026г.
Председатель ПЦК

 К.С. Кондрашова
подпись

СОДЕРЖАНИЕ

1.	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2.	СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
3.	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	8
4.	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	9

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы:

Рабочая программа учебной дисциплины ОП.11 Безопасность жизнедеятельности в цифровой среде является частью образовательной программы в соответствии с ФГОС СПО по специальности 38.02.02 Страховой дело (по отраслям).

1.2. Цель и планируемые результаты освоения учебной дисциплины:

Умения	Знания
У-1 пользоваться нормативными документами противодействию технической разведке; У-2 оценивать качество готового программного обеспечения; У-3 владеть методами и средствами технической защиты информации; У-4 методами расчета и инструментального контроля показателей технической защиты информации.	З-1 средства и методы предотвращения и обнаружения вторжений; З-2 технические каналы утечки информации; З-3 возможности технических средств перехвата информации; З-4 способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; З-5 организацию защиты информации от утечки по техническим каналам на объектах информатизации.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы	36
Суммарная учебная нагрузка во взаимодействии с преподавателем	36
в том числе:	
теоретическое обучение	10
лабораторные занятия	-
практические занятия	26
курсовая работа (проект)	-
самостоятельная работа (индивидуальный проект)	-
Промежуточная аттестация проводится в форме: зачет	

2.1. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Коды знаний и умений, формированию которых способствуют элементы программы
1	2	3	4
Тема 1. Информационная безопасность в условиях функционирования в России глобальных сетей	Содержание учебного материала	2	У-1-3 3-1-4
	1. Стандарты в области информационной безопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность		
	Практические занятия:	2	
	1. Практическое занятие № 1. Составление кластера «Международные стандарты информационного обмена»	2	
Тема 2. Нарушения и защита информационной системы	Содержание учебного материала	2	У-1-3 3-1-4
	1. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация		
	Практические занятия:	2	
	1. Практическое занятие № 2. Составление алгоритма выявления возможных нарушений информационной системы и защиты	2	
Тема 3. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	Содержание учебного материала	2	У-1-3 3-1-4
	1. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны		
	Практические занятия:	2	
	1. Практическое занятие № 3. Составление положения о коммерческой тайне компании	2	
Тема 4. Основные положения теории информационной безопасности. Модели безопасности и их	Содержание учебного материала	2	У-1-3 3-1-4
	1. Основные положения теории информационной безопасности. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании. Модели		

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся		Объем часов	Коды знаний и умений, формированию которых способствуют элементы программы
1	2		3	4
применение		безопасности для домашней информационной системы. Применение методов информационной безопасности		
	Практические занятия:		16	
	1.	Практическое занятие № 4. Анализ применимости моделей безопасности в конкретный ситуациях	2	
Тема 5. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	2.	Практическое занятие № 5. Построение таксономии нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	2	У-1-3 3-1-4
	3.	Практическое занятие № 6. Анализ способов нарушений информационной безопасности	2	
Тема 6. Использование защищенных компьютерных систем	4.	Практическое занятие № 7. Моделирование использования защищенных компьютерных систем в конкретной ситуации	2	
Тема 7. Методы криптографии	5.	Практическое занятие № 8. Анализ методов криптографии	2	У-1-3 3-1-4
	6.	Практическое занятие № 9. Анализ методов криптографии	2	
Тема 8. Основные технологии построения защищенных систем	7.	Практическое занятие № 10. Анализ применимости различных программных пакетов обеспечения безопасности в конкретной ситуации	2	
	8.	Практическое занятие № 11. Классифицирование технологий построения защищенных систем	2	
Тема 9. Место информационной безопасности экономических систем в национальной	Содержание учебного материала		2	У-1-3 3-1-4
	1.	Информационная безопасность компании. Защита экономической системы. Обмен конфиденциальной информацией. Важность защиты экономической информации и персональных данных		

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся		Объем часов	Коды знаний и умений, формированию которых способствуют элементы программы
1	2		3	4
безопасности компании		сотрудников и клиентов. Электронные деньги и безопасность финансовых переводов. Концепция информационной безопасности. Основные сведения и положения		
	Практические занятия:		4	
	1.	Практическое занятие № 12. Анализ практической /производственной ситуации	2	
	2.	Практическое занятие № 13. Анализ практической /производственной ситуации	2	
Промежуточная аттестация (зачет)				
Итого			36	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Для реализации рабочей программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Реализация программы учебной дисциплины предполагает наличие кабинета социально-экономических дисциплин, оснащенного столом преподавателя – 1 шт.; стулом преподавателя – 1 шт.; столами компьютерными – 13 шт.; креслами компьютерными – 13 шт.; столами ученическими – 12 шт.; стульями ученическими – 25 шт.; доской меловой – 1 шт.; доской интерактивной – 1 шт.; проектором – 1 шт.; моноблоками – 13 шт.; МФУ – 1 шт.; шкафом для документов – 1 шт.; шкафом архивным – 1 шт.; огнетушителем -1 шт.

3.2 Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1 Основные источники:

1. Станкевич, Л. А. Интеллектуальные системы и технологии : учебник и практикум для среднего профессионального образования / Л. А. Станкевич. - 2-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2025. - 478 с. - (Профессиональное образование). - ISBN 978-5-534-20364-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566524> (дата обращения: 06.11.2025).с.

3.2.2 Дополнительные источники

1. Иванов, В. М. Интеллектуальные системы : учебное пособие для среднего профессионального образования / В. М. Иванов ; под научной редакцией А. Н. Сесекина. - Москва : Издательство Юрайт, 2025. - 88 с. - (Профессиональное образование). - ISBN 978-5-534-20852-8. - Текст : электронный // Образовательная платформа Юрайт [сайт]. - URL: <https://urait.ru/bcode/558866> (дата обращения: 06.11.2025).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: 3-1 средства и методы предотвращения и обнаружения вторжений; 3-2 технические каналы утечки информации; 3-3 возможности технических средств перехвата информации; 3-4 способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; 3-5 организацию защиты информации от утечки по техническим каналам на объектах информатизации	- называет средства и методы предотвращения и обнаружения вторжений; - характеризует технические каналы утечки информации; возможности технических средств перехвата информации; - перечисляет способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - характеризует организацию защиты информации от утечки по техническим каналам на объектах информатизации.	Текущий контроль: оценка результатов ответов, собеседования. Оценка выполнения тестового задания. Промежуточная аттестация: оценка выполнения задания на зачете.
Умения: У-1 пользоваться нормативными документами противодействию технической разведке; У-2 оценивать качество готового программного обеспечения; У-3 владеть методами и средствами технической защиты информации; У-4 методами расчета и инструментального контроля показателей технической защиты информации.	- пользуется нормативными актами, способствующими противодействию технической разведке; оценивает качество готового программного обеспечения; - владеет методами и средствами технической защиты информации; - использует методы расчета и инструментального контроля показателей технической защиты информации.	Текущий контроль: оценка результатов ответов, собеседования. Оценка выполнения тестового задания. Промежуточная аттестация: оценка выполнения задания на зачете.