Министерство образования Иркутской области
Государственное бюджетное профессиональное образовательное учреждение Иркутской области
«Иркутский авиационный техникум»

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»
_____ Якубовский А.Н.
«08» февраля 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.19 Безопасность информационных систем

специальности

09.02.07 Информационные системы и программирование

Иркутск, 2023

Рассмотрена
цикловой комиссией
ИСП протокол №9 от
17.05.2023 г.

Рабочая программа разработана на основе ФГОС СПО специальности 09.02.07 Информационные системы и программирование; учебного плана специальности 09.02.07 Информационные системы и программирование; на основе рекомендаций работодателя (протокол заседания ВЦК ИСП №8 от 30.03.2023 г.).

№	Разработчик ФИО
1	Огородникова Наталья Романовна

СОДЕРЖАНИЕ

		стр.
1	ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	4
2	СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	6
3	УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	13
4	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	15

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.19 БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

1.1. Область применения рабочей программы (РП)

РП является частью программы подготовки специалистов среднего звена по специальности 09.02.07 Информационные системы и программирование.

1.2. Место дисциплины в структуре ППССЗ:

ОП.00 Общепрофессиональный цикл.

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

Результаты освоения дисциплины	№ результата	Формируемый результат
Знать	1.1	основные принципы и концепции безопасности информационных систем
	1.2	различные виды угроз и атак на информационные системы
	1.3	методы и средства защиты информации
Уметь	2.1	анализировать угрозы и риски для информационных систем
	2.2	разрабатывать стратегии и планы по обеспечению безопасности информационных систем
	2.3	применять методы и средства защиты информации в информационных системах
Личностные результаты реализации программы воспитания	3.1	Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации
	3.2	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
	3.3	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

	3.4	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

1.4. Формируемые компетенции:

ОК.1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК.2 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК.3 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК.4 Эффективно взаимодействовать и работать в коллективе и команде
ОК.5 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК.9 Пользоваться профессиональной документацией на государственном и иностранном языках
ПК.5.3 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием
ПК.7.5 Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации

1.5. Количество часов на освоение программы дисциплины:
Общий объем дисциплины 74 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Виды учебной работы	Объем часов
Общий объем дисциплины	**74**
Работа обучающихся во взаимодействии с преподавателем:	**72**
теоретическое обучение	36
лабораторные занятия	0
практические занятия	24
консультация	6
Промежуточная аттестация в форме "Экзамен" (семестр 5)	6
Самостоятельная работа студентов	**2**

2.2.Тематический план и содержание дисциплины

Наименование разделов	Наименование темы теоретического обучения, практических и лабораторных занятий, самостоятельной работы, консультаций, курсового проекта (работы)	Объём часов	Формируемые результаты: знать, уметь, личностные результаты реализации программы воспитания	Формируемые компетенции	Текущий контроль
1	2	3	4	5	6
Раздел 1	**Введение в информационную безопасность**	**16**			
Тема 1.1	**Сущность и понятие информационной безопасности**	**4**			
Занятие 1.1.1 теория	Основные понятия информационной безопасности.	2	1.1, 2.1	ОК.1	
Занятие 1.1.2 теория	Анализ угроз информационной безопасности.	2	1.1, 2.1, 3.1	ОК.2	
Тема 1.2	**Информационная безопасность РФ**	**8**			
Занятие 1.2.1 теория	Информационная безопасность в системе национальной безопасности Российской Федерации.	2	2.1, 2.2	ОК.3	
Занятие 1.2.2 теория	Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.	2	1.1, 2.2	ОК.1, ОК.2	
Занятие 1.2.3 теория	Основные положения государственной информационной политики России.	2	1.3, 2.1, 2.2, 2.3	ОК.9	
Занятие 1.2.4 практическое занятие	Доктрина информационной безопасности Российской Федерации.	1	1.1, 1.3, 2.1, 2.2, 2.3	ОК.3	

Занятие 1.2.5 практическое занятие	Анализ Доктрины информационной безопасности Российской Федерации.	1	1.3, 2.1, 2.2, 2.3	ОК.9	1.1, 2.2
Тема 1.3	**Разновидности атак на защищаемые ресурсы**	**4**			
Занятие 1.3.1 теория	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.	2	1.3, 2.1	ОК.1, ОК.3	
Занятие 1.3.2 теория	Методы оценки уязвимости информации. Виды утечки информации.	2	1.3, 2.1, 2.3	ОК.9	
Раздел 2	**Источники и носители защищаемой информации**	**12**			
Тема 2.1	**Конфиденциальная информация**	**12**			
Занятие 2.1.1 теория	Понятие конфиденциальной информации.	2	1.3, 2.1, 2.2	ОК.9	
Занятие 2.1.2 практическое занятие	Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.	2	1.3, 2.1, 2.2	ОК.2	
Занятие 2.1.3 теория	Жизненные циклы конфиденциальной информации.	2	2.3	ОК.9	
Занятие 2.1.4 теория	Защита информации составляющей государственную тайну.	2	2.2, 3.4	ОК.1	
Занятие 2.1.5 теория	Защита информации, охраняемая авторским и патентным правом.	2	2.3	ОК.3, ОК.9	
Занятие 2.1.6 Самостоятельная работа	Анализ защищенности объекта защиты информации.	2	2.3	ОК.2	
Раздел 3	**Средства и способы обеспечения информационной безопасности**	**40**			
Тема 3.1	**Защита от несанкционированного доступа, модели и основные принципы защиты информации**	**13**			

Занятие 3.1.1 практическое занятие	Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД).	2	, 2.3	ОК.3	
Занятие 3.1.2 практическое занятие	Стандарты в области информационной безопасности АСОД.	2	2.3	ОК.9	
Занятие 3.1.3 практическое занятие	Показатели защищенности СВТ. Защита информации в АСОД.	2	2.3	ОК.2	
Занятие 3.1.4 практическое занятие	Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.	1	1.2, 2.3	ОК.3	1.1, 2.3
Занятие 3.1.5 практическое занятие	Автоматизированная система, как объект информационной защиты.	1	1.3, 2.3	ОК.2	
Занятие 3.1.6 практическое занятие	Основные методы и приемы защиты от несанкционированного доступа.	2	2.3, 3.3	ОК.2	
Занятие 3.1.7 практическое занятие	Методы и средства защиты информации.	2	2.3	ОК.3	
Занятие 3.1.8 практическое занятие	Средства и способы обеспечения информационной безопасности.	1	1.3, 2.1	ОК.9	1.3, 2.1
Тема 3.2	**Компьютерные вирусы и антивирусные программы**	**4**			
Занятие 3.2.1 теория	Проблема вирусного заражения программ. Классификация вирусов. Способы заражения программ.	2	1.3, 2.3	ОК.4, ОК.5	

Занятие 3.2.2 практическое занятие	Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ.	2	2.3	ОК.1	
Тема 3.3	**Технология обнаружения вторжения**	**23**			
Занятие 3.3.1 практическое занятие	Адаптивное управление безопасностью.	2	2.1, 2.3	ОК.2	
Занятие 3.3.2 практическое занятие	Средства анализа защищенности сетевых протоколов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.	2	2.1, 2.3	ОК.9	
Занятие 3.3.3 практическое занятие	Методы анализа сетевой информации.	1	1.3, 2.3	ОК.2, ПК.5.3	1.2, 2.2
Занятие 3.3.4 теория	Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.	2	1.3, 2.3	ОК.9	
Занятие 3.3.5 теория	Основы сетевого и межсетевого взаимодействия.	2	2.3	ОК.2	
Занятие 3.3.6 теория	Технологии межсетевых экранов. Требования и показатели защищенности межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.	2	1.3, 2.3	ОК.3, ПК.5.3	
Занятие 3.3.7 теория	Политика безопасности. Сетевая политика безопасности.	2	1.3, 2.1	ОК.3	
Занятие 3.3.8 теория	Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности обнаружения атак на сетевом и операционном уровне. Реагирование на атаку.	1	1.3, 2.3	ОК.9	
Занятие 3.3.9 теория	Обзор современных средств обнаружения атак.	1	1.3, 2.3, 3.2	ОК.2	

Занятие 3.3.10 теория	Анализ защищенности объекта защиты информации.	1	2.1, 2.3	ОК.1, ПК.7.5	1.1, 2.3
Занятие 3.3.11 теория	Построение модели потенциального нарушителя информационной системы.	1	1.3, 2.3	ОК.3	
Занятие 3.3.12 консультация	Методы и средства защиты информации.	2	1.3	ОК.1, ПК.5.3	
Занятие 3.3.13 консультация	Виды угроз и атак на информационные системы.	2	1.2	ОК.4, ПК.5.3, ПК.7.5	
Занятие 3.3.14 консультация	Принципы и концепции безопасности информационных систем.	2	1.1	ОК.1, ОК.9, ПК.5.3	
	Экзамен	6			
	ВСЕГО:	74			

2.3. Формирование личностных результатов реализации программы воспитания

Наименование темы занятия	Наименование личностного результата реализации программы воспитания	Тип мероприятия	Наименование мероприятия
1.1.2 Анализ угроз информационной безопасности.	3.1 Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации	Беседа	Значимость дисциплины на государственном уровне

2.1.4 Защита информации составляющей государственную тайну.	3.4 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	Дискуссия	Способы защиты конфиденциальной информации
3.1.1 Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД).		Дебаты	Интегральная безопасность
3.1.6 Основные методы и приемы защиты от несанкционированного доступа.	3.3 Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм	Конференция	Ценность жизни, здоровья и безопасности
3.3.9 Обзор современных средств обнаружения атак.	3.2 Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации	Викторина	Обзор современных средств обнаружения атак

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета: Лаборатория организации и принципов построения информационных систем.

ОБЕСПЕЧЕННОСТЬ ВСЕХ ВИДОВ ЛАБОРАТОРНЫХ РАБОТ И ПРАКТИЧЕСКИХ ЗАНЯТИЙ (далее – ЛПР)

Наименование занятия ЛПР	Перечень оборудования
1.2.4 Доктрина информационной безопасности Российской Федерации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010
1.2.5 Анализ Доктрины информационной безопасности Российской Федерации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office Professional Plus 2019
2.1.2 Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.1 Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД).	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.2 Стандарты в области информационной безопасности АСОД.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.3 Показатели защищенности СВТ. Защита информации в АСОД.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.4 Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.5 Автоматизированная система, как объект информационной защиты.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.6 Основные методы и приемы защиты от несанкционированного доступа.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор

3.1.7 Методы и средства защиты информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.8 Средства и способы обеспечения информационной безопасности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.2.2 Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.1 Адаптивное управление безопасностью.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.2 Средства анализа защищенности сетевых протоколов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.3 Методы анализа сетевой информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Visual Studio, Плазменный телевизор

3.2. Информационное обеспечение реализации программы

Перечень рекомендуемых учебных, учебно-методических печатных и/или электронных изданий, нормативных и нормативно-технических документов

№	**Библиографическое описание**	**Тип (основной источник, дополнительный источник, электронный ресурс)**

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины проводится на основе заданий и критериев их оценивания, представленных в фондах оценочных средств по дисциплине ОП.19 Безопасность информационных систем. Фонды оценочных средств содержат контрольно-оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации.

4.1. Текущий контроль успеваемости

Текущий контроль успеваемости осуществляется преподавателем в процессе проведения теоретических занятий, практических занятий, лабораторных работ, курсового проектирования.

Результаты обучения (освоенные умения, усвоенные знания)	Индекс темы занятия
Текущий контроль № 1 (45 минут). **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Проверочная работа	
1.1 основные принципы и концепции безопасности информационных систем	1.1.1, 1.1.2, 1.2.2, 1.2.4
2.2 разрабатывать стратегии и планы по обеспечению безопасности информационных систем	1.2.1, 1.2.2, 1.2.3, 1.2.4
Текущий контроль № 2 (45 минут). **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Проверочная работа	
1.1 основные принципы и концепции безопасности информационных систем	
2.3 применять методы и средства защиты информации в информационных системах	1.2.3, 1.2.4, 1.2.5, 1.3.2, 2.1.3, 2.1.5, 2.1.6, 3.1.1, 3.1.2, 3.1.3
Текущий контроль № 3 (45 минут). **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Проверочная работа	
1.3 методы и средства защиты информации	1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 2.1.1, 2.1.2, 3.1.5
2.1 анализировать угрозы и риски для информационных систем	1.1.1, 1.1.2, 1.2.1, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 2.1.1, 2.1.2
Текущий контроль № 4 (45 минут). **Методы и формы:** Лабораторная работа (Опрос) **Вид контроля:**	

1.2 различные виды угроз и атак на информационные системы	3.1.4
2.2 разрабатывать стратегии и планы по обеспечению безопасности информационных систем	1.2.5, 2.1.1, 2.1.2, 2.1.4
Текущий контроль № 5 (45 минут). **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Проверочная работа	
1.1 основные принципы и концепции безопасности информационных систем	
2.3 применять методы и средства защиты информации в информационных системах	3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.2.1, 3.2.2, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.3.6, 3.3.8, 3.3.9

4.2. Промежуточная аттестация

№ семестра	Вид промежуточной аттестации
5	Экзамен

Экзамен может быть выставлен автоматически по результатам текущих контролей
Текущий контроль №1
Текущий контроль №2
Текущий контроль №3
Текущий контроль №4
Текущий контроль №5

Методы и формы: Письменный опрос (Опрос)
Описательная часть: По выбору выполнить 1 теоретическое задание и 1 практическое задание

Результаты обучения (освоенные умения, усвоенные знания)	Индекс темы занятия
1.1 основные принципы и концепции безопасности информационных систем	1.1.1, 1.1.2, 1.2.2, 1.2.4, 3.3.14
1.2 различные виды угроз и атак на информационные системы	3.1.4, 3.3.13

1.3 методы и средства защиты информации	1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 2.1.1, 2.1.2, 3.1.5, 3.1.8, 3.2.1, 3.3.3, 3.3.4, 3.3.6, 3.3.7, 3.3.8, 3.3.9, 3.3.11, 3.3.12
2.2 разрабатывать стратегии и планы по обеспечению безопасности информационных систем	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 2.1.1, 2.1.2, 2.1.4
2.1 анализировать угрозы и риски для информационных систем	1.1.1, 1.1.2, 1.2.1, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 2.1.1, 2.1.2, 3.1.8, 3.3.1, 3.3.2, 3.3.7, 3.3.10
2.3 применять методы и средства защиты информации в информационных системах	1.2.3, 1.2.4, 1.2.5, 1.3.2, 2.1.3, 2.1.5, 2.1.6, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.2.1, 3.2.2, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.3.6, 3.3.8, 3.3.9, 3.3.10, 3.3.11

4.3. Критерии и нормы оценки результатов освоения дисциплины

Для каждой дидактической единицы представлены показатели оценивания на «3», «4», «5» в фонде оценочных средств по дисциплине.

Оценка «2» ставится в случае, если обучающийся полностью не выполнил задание, или выполненное задание не соответствует показателям на оценку «3».