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

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»
_____ Якубовский А.Н.
«29» мая 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.05 Основы информационной безопасности

специальности

09.02.11 Разработка и управление программным обеспечением

Иркутск, 2026

Рассмотрена
цикловой комиссией

Рабочая программа разработана на основе ФГОС СПО специальности 09.02.11 Разработка и управление программным обеспечением; учебного плана специальности 09.02.11 Разработка и управление программным обеспечением; с учетом примерной рабочей программы учебной дисциплины "Основы информационной безопасности" в составе примерной образовательной программы специальности 09.02.11 Разработка и управление программным обеспечением, утвержденной протоколом Федерального учебно-методического объединения по УГПС 09.00.00 от 01.09.2025 № 7/2025 (Приказ ФГБОУ ДПО ИРПО № 01-09-580/2025 от 13.10.2025).

№	Разработчик ФИО
1	Бодоев Даниил Александрович

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения рабочей программы (РП)

РП является частью программы подготовки специалистов среднего звена по специальности 09.02.11 Разработка и управление программным обеспечением.

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	Понятия информационной безопасности: информационная безопасность, конфиденциальность информации, политика безопасности, риск, уязвимость
	1.2	Классификацию угроз информационной безопасности
	1.3	Нормативно-правовые акты информационной безопасности
	1.4	Организационные средства защиты информации
	1.5	Технические средства защиты информации
Уметь	2.1	Анализировать угрозы и риски информационной безопасности
	2.2	Выбирать и применять методы защиты информации

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
ПК.3.5 Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности

1.5. Количество часов на освоение программы дисциплины:

Общий объем дисциплины 32 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Виды учебной работы	Объем часов
Общий объем дисциплины	**32**
Работа обучающихся во взаимодействии с преподавателем:	**30**
теоретическое обучение	14
лабораторные занятия	0
практические занятия	16
Промежуточная аттестация в форме "Дифференцированный зачет" (семестр 4)	0
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	**Основы информационной безопасности**	**32**			
Тема 1.1	**Понятия информационной безопасности**	**4**			
Занятие 1.1.1 теория	Основные понятия информационной безопасности.	2	1.1	ОК.1, ОК.2, ПК.3.5	
Занятие 1.1.2 теория	Нормативно-правовая база информационной безопасности.	2	1.3	ОК.1, ОК.2, ПК.3.5	
Тема 1.2	**Классификация угроз информационной безопасности и средства защиты информации**	**14**			
Занятие 1.2.1 теория	Виды и классификация угроз информационной безопасности.	2	1.2	ОК.1, ОК.2, ПК.3.5	
Занятие 1.2.2 практическое занятие	Методы анализа угроз информационной безопасности.	2	2.1	ОК.1, ОК.2, ПК.3.5	
Занятие 1.2.3 теория	Организационные средства защиты информации.	2	1.4	ОК.1, ОК.2, ПК.3.5	
Занятие 1.2.4 теория	Выбор организационных мер защиты информации.	1	1.4	ОК.1, ОК.2, ПК.3.5	

Занятие 1.2.5 теория	Выбор организационных мер защиты информации.	1	1.4	ОК.1, ОК.2, ПК.3.5	1.1, 1.2, 1.3, 1.4
Занятие 1.2.6 теория	Технические средства защиты информации.	2	1.5	ОК.1, ОК.2, ПК.3.5	
Занятие 1.2.7 практическое занятие	Комплексное применение средств защиты информации.	2	1.5, 2.2	ОК.1, ОК.2, ПК.3.5	
Занятие 1.2.8 практическое занятие	Выбор технических средств защиты информации.	2	1.5	ОК.1, ОК.2, ПК.3.5	
Тема 1.3	**Анализ угроз и рисков**	**4**			
Занятие 1.3.1 практическое занятие	Количественная и качественная оценка рисков информационной безопасности.	2	2.1	ОК.1, ОК.2, ПК.3.5	
Занятие 1.3.2 практическое занятие	Разработка мер реагирования на риски (план обработки рисков).	2	2.1	ОК.1, ОК.2, ПК.3.5	
Тема 1.4	**Применение методов защиты**	**10**			
Занятие 1.4.1 теория	Обоснование выбора методов защиты информации.	2	1.2, 2.2	ОК.1, ОК.2, ПК.3.5	
Занятие 1.4.2 практическое занятие	Обоснование выбора методов защиты информации.	2	1.2, 2.2	ОК.1, ОК.2, ПК.3.5	
Занятие 1.4.3 Самостоятельная работа	Комплексный анализ безопасности информационной системы	2	1.3, 1.5, 2.1	ОК.1, ОК.2, ПК.3.5	
Занятие 1.4.4 практическое занятие	Построение и оценка эффективности системы защиты информации.	2	1.4, 1.5, 2.2	ОК.1, ОК.2, ПК.3.5	

Занятие 1.4.5 практическое занятие	Построение и оценка эффективности системы защиты информации.	1	2.2	ОК.1, ОК.2, ПК.3.5	
Занятие 1.4.6 практическое занятие	Построение и оценка эффективности системы защиты информации.	1	2.2	ОК.1, ОК.2, ПК.3.5	1.5, 2.1, 2.2
	ВСЕГО:	32			

2.3. Формирование личностных результатов реализации программы воспитания

Наименование темы занятия	Наименование личностного результата реализации программы воспитания	Тип мероприятия	Наименование мероприятия

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета: Лаборатория компьютерных сетей и основ информационной безопасности.

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

Наименование занятия ЛПР	**Перечень оборудования**
1.2.2 Методы анализа угроз информационной безопасности.	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)
1.2.7 Комплексное применение средств защиты информации.	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)
1.2.8 Выбор технических средств защиты информации.	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)
1.3.1 Количественная и качественная оценка рисков информационной безопасности.	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)
1.3.2 Разработка мер реагирования на риски (план обработки рисков).	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)
1.4.2 Обоснование выбора методов защиты информации.	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)

1.4.4 Построение и оценка эффективности системы защиты информации.	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)
1.4.5 Построение и оценка эффективности системы защиты информации.	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)
1.4.6 Построение и оценка эффективности системы защиты информации.	Персональный компьютер, Microsoft Windows 10, Microsoft Office 2010, Yandex Browser, Комплект презентационного оборудования (Интерактивная доска TeachTouch)

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.05 Основы информационной безопасности. 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:** Тестирование (Опрос) **Вид контроля:** Письменная работа	
1.1 Понятия информационной безопасности: информационная безопасность, конфиденциальность информации, политика безопасности, риск, уязвимость	1.1.1
1.2 Классификацию угроз информационной безопасности	1.2.1
1.3 Нормативно-правовые акты информационной безопасности	1.1.2
1.4 Организационные средства защиты информации	1.2.3, 1.2.4
Текущий контроль № 2 (45 минут). **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Письменная работа	
1.5 Технические средства защиты информации	1.2.6, 1.2.7, 1.2.8, 1.4.3, 1.4.4
2.1 Анализировать угрозы и риски информационной безопасности	1.2.2, 1.3.1, 1.3.2, 1.4.3
2.2 Выбирать и применять методы защиты информации	1.2.7, 1.4.1, 1.4.2, 1.4.4, 1.4.5

4.2. Промежуточная аттестация

№ семестра	Вид промежуточной аттестации
4	Дифференцированный зачет

Дифференцированный зачет может быть выставлен автоматически по результатам текущих контролей
Текущий контроль №1
Текущий контроль №2

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 Понятия информационной безопасности: информационная безопасность, конфиденциальность информации, политика безопасности, риск, уязвимость	1.1.1
1.2 Классификацию угроз информационной безопасности	1.2.1, 1.4.1, 1.4.2
1.3 Нормативно-правовые акты информационной безопасности	1.1.2, 1.4.3
1.4 Организационные средства защиты информации	1.2.3, 1.2.4, 1.2.5, 1.4.4
1.5 Технические средства защиты информации	1.2.6, 1.2.7, 1.2.8, 1.4.3, 1.4.4
2.1 Анализировать угрозы и риски информационной безопасности	1.2.2, 1.3.1, 1.3.2, 1.4.3
2.2 Выбирать и применять методы защиты информации	1.2.7, 1.4.1, 1.4.2, 1.4.4, 1.4.5, 1.4.6

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».