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

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»
_____ Якубовский А.Н.
«30» мая 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.16 Безопасность информационных систем

специальности

09.02.07 Информационные системы и программирование

Иркутск, 2025

Рассмотрена
цикловой комиссией
ИСП-ИС протокол № 11 от
22.05.2024 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-ИС № 9 от 13.03.2024 г.).

№	Разработчик ФИО
1	Бодоев Даниил Александрович

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.16 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
	1.4	нормативно-правовая база в области информационной безопасности
	1.5	технологии мониторинга и аудита безопасности
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, средства защиты информации и нормативные документы при проектировании и обеспечении безопасности информационных систем
	2.4	проводить аудит систем безопасности баз данных и серверов
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
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	**Основы информационной безопасности**	**12**			
Тема 1.1	**Принципы и концепции информационной безопасности**	**4**			
Занятие 1.1.1 теория	Основные понятия информационной безопасности.	2	1.1, 3.2	ОК.1, ПК.5.3	
Занятие 1.1.2 теория	Классификация объектов защиты	2	1.1, 2.1	ОК.1, ПК.5.3	
Тема 1.2	**Виды угроз и атак**	**4**			
Занятие 1.2.1 теория	Классификация угроз (физические, программные, сетевые)	2	1.2, 2.2	ОК.1, ОК.2, ПК.5.3	
Занятие 1.2.2 теория	Вредоносное программное обеспечение	1	1.2, 2.2	ОК.1, ОК.2, ПК.5.3	
Занятие 1.2.3 теория	Вредоносное программное обеспечение	1	1.1, 2.1	ОК.1, ПК.5.3	1.1, 2.1
Тема 1.3	**Классификация методов защиты информации**	**4**			
Занятие 1.3.1 теория	Основные стратегии защиты данных	2	1.3, 2.2	ОК.1, ОК.4, ПК.5.3, ПК.7.5	

Занятие 1.3.2 теория	Аппаратные и программные средства защиты	2	1.2, 2.1	ОК.1, ОК.2, ПК.5.3	
Раздел 2	**Нормативно-правовая база**	**6**			
Тема 2.1	**Законодательство РФ по информационной безопасности**	**6**			
Занятие 2.1.1 теория	152-ФЗ "О персональных данных", ГОСТ Р 57580	2	1.4	ОК.3, ПК.5.3	
Занятие 2.1.2 практическое занятие	Основные положения, стратегия РФ в сфере информационной безопасности	2	2.3, 3.3	ОК.2, ОК.3, ПК.5.3	
Занятие 2.1.3 теория	Ответственность за нарушения в сфере информационной безопасности	1	1.4	ОК.3, ПК.5.3	
Занятие 2.1.4 теория	Ответственность за нарушения в сфере информационной безопасности	1	1.4, 2.3	ОК.2, ОК.3, ПК.5.3	1.4, 2.2
Раздел 3	**Методы и средства защиты**	**50**			
Тема 3.1	**Криптография**	**6**			
Занятие 3.1.1 теория	Шифрование (AES, RSA)	2	1.3, 2.3	ОК.2, ОК.3, ОК.4, ПК.5.3, ПК.7.5	
Занятие 3.1.2 теория	Шифрование (цифровые подписи)	2	1.3, 2.3	ОК.2, ОК.3, ОК.4, ПК.5.3, ПК.7.5	
Занятие 3.1.3 практическое занятие	Генерация ключей, шифрование сообщений в OpenSSL	2	1.3, 2.3, 3.1	ОК.2, ОК.3, ОК.4, ПК.5.3, ПК.7.5	
Тема 3.2	**Защита на уровне ОС, сетевые экраны, антивирусное ПО**	**4**			
Занятие 3.2.1 практическое занятие	Настройка межсетевого экрана	2	1.3, 2.4	ОК.2, ОК.4, ПК.7.5	

Занятие 3.2.2 Самостоятельная работа	Анализ логов антивирусного ПО	2	1.3, 2.1	ОК.1, ОК.4, ПК.5.3, ПК.7.5	
Тема 3.3	**Аудит безопасности**	**8**			
Занятие 3.3.1 теория	Защита на уровне ОС, сетевые экраны, антивирусное ПО	1	1.3, 2.1	ОК.1, ОК.4, ПК.5.3, ПК.7.5	1.3, 2.3
Занятие 3.3.2 теория	Инструменты аудита (metasploit)	1	1.5, 2.4	ОК.2, ПК.7.5	
Занятие 3.3.3 теория	Инструменты аудита (Nmap)	2	1.5, 2.4	ОК.2, ПК.7.5	
Занятие 3.3.4 практическое занятие	Проведение тестирования безопасности системы (metasploit)	2	1.5, 2.4, 3.4	ОК.2, ПК.7.5	
Занятие 3.3.5 практическое занятие	Проведение тестирования безопасности системы (Nmap)	2	1.5, 2.4	ОК.2, ПК.7.5	
Тема 3.4	**SIEM-системы и анализ логов**	**8**			
Занятие 3.4.1 теория	Анализ сетевого трафика	2	1.4, 2.4	ОК.2, ОК.3, ПК.5.3, ПК.7.5	
Занятие 3.4.2 теория	Анализ журналов событий	2	1.4, 2.4	ОК.2, ОК.3, ПК.5.3, ПК.7.5	
Занятие 3.4.3 практическое занятие	Анализ логов в Splunk	2	1.5, 2.4	ОК.2, ПК.7.5	
Занятие 3.4.4 практическое занятие	Анализ логов Fluentd	2	2.1, 2.4	ОК.1, ОК.2, ПК.5.3, ПК.7.5	
Тема 3.5	**Защита баз данных**	**8**			

Занятие 3.5.1 теория	SIEM-системы и анализ логов	1	1.5, 2.4	ОК.2, ПК.7.5	1.2, 2.4
Занятие 3.5.2 теория	SQL-инъекции	1	1.5, 2.4	ОК.2, ПК.7.5	
Занятие 3.5.3 теория	Управления доступом к ресурсам (RBAC)	2	1.5, 2.4	ОК.2, ПК.7.5	
Занятие 3.5.4 практическое занятие	Выполнение SQL-инъекций	2	1.5, 2.4, 3.1	ОК.2, ПК.7.5	
Занятие 3.5.5 практическое занятие	Управление доступом на основе ролей (RBAC)	2	1.5, 2.4	ОК.2, ПК.7.5	
Тема 3.6	**Защита серверов**	**6**			
Занятие 3.6.1 теория	Настройка Firewall, защита от DDos	2	1.5, 2.4	ОК.2, ПК.7.5	
Занятие 3.6.2 практическое занятие	Настройка Firewall	2	1.5, 2.4	ОК.2, ПК.7.5	
Занятие 3.6.3 практическое занятие	Настройка Защиты от DDos	2	1.5, 2.4	ОК.2, ПК.7.5	
Тема 3.7	**Разработка политики безопасности**	**4**			
Занятие 3.7.1 теория	Защита серверов и баз данных	1	1.5, 2.4	ОК.2, ПК.7.5	1.5, 2.4
Занятие 3.7.2 теория	Написание плана реагирования на инциденты	1	1.5, 2.4	ОК.2, ПК.7.5	

Занятие 3.7.3 практическое занятие	Написание плана реагирования на инциденты	2	1.5, 2.2	ОК.1, ОК.2, ПК.5.3, ПК.7.5	
Тема 3.8	**Консультации**	**6**			
Занятие 3.8.1 консультация	Подготовка к промежуточным тестам	2	2.3, 2.4	ОК.2, ОК.3, ПК.5.3, ПК.7.5	
Занятие 3.8.2 консультация	Разбор сложных тем (SIEM, аудит, криптография)	2	2.1, 2.2	ОК.1, ПК.5.3	
Занятие 3.8.3 консультация	Разработка политики безопасности	2	1.2, 2.2	ОК.1, ОК.2, 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
1.1.1 Основные понятия информационной безопасности.	3.2 Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации	Беседа	Информационная безопасность: основы профессии
2.1.2 Основные положения, стратегия РФ в сфере информационной безопасности	3.3 Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм	Диспут	Способы защиты конфиденциальной информации

3.1.3 Генерация ключей, шифрование сообщений в OpenSSL	3.1 Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации	Беседа	Тайны криптографии: шифруем как профессионалы
3.3.4 Проведение тестирования безопасности системы (metasploit)	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	Деловая игра	Киберучения: проверка защиты на практике
3.5.4 Выполнение SQL-инъекций	3.1 Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации	Мини-проект	Атака и защита: разбираем реальные случаи SQL-инъекций

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**
2.1.2 Основные положения, стратегия РФ в сфере информационной безопасности	Персональный компьютер, Операционная система Microsoft Windows 10 Pro, Yandex Browser, Microsoft Office Professional Plus 2019
3.1.3 Генерация ключей, шифрование сообщений в OpenSSL	Персональный компьютер, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro
3.2.1 Настройка межсетевого экрана	Персональный компьютер, Oracle VM VirtualBox, Yandex Browser
3.3.4 Проведение тестирования безопасности системы (metasploit)	Персональный компьютер, Microsoft SQL Server, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro
3.3.5 Проведение тестирования безопасности системы (Nmap)	Персональный компьютер, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro, Yandex Browser, Microsoft Office Professional Plus 2019
3.4.3 Анализ логов в Splunk	Персональный компьютер, OpenOffice, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro
3.4.4 Анализ логов Fluentd	Персональный компьютер, Операционная система Microsoft Windows 10 Pro, Yandex Browser, Microsoft Office Professional Plus 2019
3.5.4 Выполнение SQL-инъекций	Персональный компьютер, MySQL Workbench, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro

3.5.5 Управление доступом на основе ролей (RBAC)	Персональный компьютер, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro, Microsoft Office Professional Plus 2019
3.6.2 Настройка Firewall	Персональный компьютер, MySQL Workbench, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro
3.6.3 Настройка Защиты от DDos	Персональный компьютер, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro, Yandex Browser, Microsoft Office Professional Plus 2019
3.7.3 Написание плана реагирования на инциденты	Персональный компьютер, Oracle VM VirtualBox, Операционная система Microsoft Windows 10 Pro, Yandex Browser

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.16 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 (30 минут). **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Письменная работа	
1.1 основные принципы и концепции безопасности информационных систем	1.1.1, 1.1.2
2.1 анализировать угрозы и риски для информационных систем	1.1.2
Текущий контроль № 2 (30 минут). **Методы и формы:** Практическая работа (Опрос) **Вид контроля:** Письменная работа	
1.4 нормативно-правовая база в области информационной безопасности	2.1.1, 2.1.3
2.2 разрабатывать стратегии и планы по обеспечению безопасности информационных систем	1.2.1, 1.2.2, 1.3.1
Текущий контроль № 3 (45 минут). **Методы и формы:** Практическая работа (Опрос) **Вид контроля:** Практическая работа с применением ИКТ	
1.3 методы и средства защиты информации	1.3.1, 3.1.1, 3.1.2, 3.1.3, 3.2.1, 3.2.2
2.3 применять методы, средства защиты информации и нормативные документы при проектировании и обеспечении безопасности информационных систем	2.1.2, 2.1.4, 3.1.1, 3.1.2, 3.1.3

Текущий контроль № 4 (45 минут). **Методы и формы:** Практическая работа (Опрос) **Вид контроля:** Практическая работа с применением ИКТ	
1.2 различные виды угроз и атак на информационные системы	1.2.1, 1.2.2, 1.3.2
2.4 проводить аудит систем безопасности баз данных и серверов	3.2.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.4.1, 3.4.2, 3.4.3, 3.4.4
Текущий контроль № 5 (45 минут). **Методы и формы:** Практическая работа (Опрос) **Вид контроля:** Практическое задание	
1.5 технологии мониторинга и аудита безопасности	3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.4.3, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, 3.6.1, 3.6.2, 3.6.3
2.4 проводить аудит систем безопасности баз данных и серверов	3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, 3.6.1, 3.6.2, 3.6.3

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
1.5 технологии мониторинга и аудита безопасности	3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.4.3, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, 3.6.1, 3.6.2, 3.6.3, 3.7.1, 3.7.2, 3.7.3

2.3 применять методы, средства защиты информации и нормативные документы при проектировании и обеспечении безопасности информационных систем	2.1.2, 2.1.4, 3.1.1, 3.1.2, 3.1.3, 3.8.1
1.4 нормативно-правовая база в области информационной безопасности	2.1.1, 2.1.3, 2.1.4, 3.4.1, 3.4.2
1.1 основные принципы и концепции безопасности информационных систем	1.1.1, 1.1.2, 1.2.3
1.2 различные виды угроз и атак на информационные системы	1.2.1, 1.2.2, 1.3.2, 3.8.3
1.3 методы и средства защиты информации	1.3.1, 3.1.1, 3.1.2, 3.1.3, 3.2.1, 3.2.2, 3.3.1
2.2 разрабатывать стратегии и планы по обеспечению безопасности информационных систем	1.2.1, 1.2.2, 1.3.1, 3.7.3, 3.8.2, 3.8.3
2.1 анализировать угрозы и риски для информационных систем	1.1.2, 1.2.3, 1.3.2, 3.2.2, 3.3.1, 3.4.4, 3.8.2
2.4 проводить аудит систем безопасности баз данных и серверов	3.2.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, 3.6.1, 3.6.2, 3.6.3, 3.7.1, 3.7.2, 3.8.1

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».