



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

УТВЕРЖДАЮ  
Директор  
ГБПОУИО «ИАТ»

\_\_\_\_\_/Семёнов В.Г.  
«31» мая 2016 г.

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

ОП.16 Безопасность информационных систем

специальности


09.02.03 Программирование в компьютерных системах

Иркутск, 2016

Рассмотрена  
цикловой комиссией

Рабочая программа разработана на основе ФГОС  
СПО специальности 09.02.03 Программирование в  
компьютерных системах; учебного плана  
специальности 09.02.03 Программирование в  
компьютерных системах.

Председатель ЦК

 /М.А. Кудрявцева /

№	Разработчик ФИО
1	Филимонова Ольга Николаевна

## СОДЕРЖАНИЕ

		стр.
1	ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	4
2	СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	6
3	УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	11
4	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	12

# 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 09.02.03 Программирование в компьютерных системах.

## 1.2. Место дисциплины в структуре ППССЗ:

ОП.00 Общепрофессиональный цикл.

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

В результате освоения дисциплины обучающийся должен	№ дидактической единицы	Формируемая дидактическая единица
Знать	1.1	Сущность и понятие информационной безопасности, характеристику ее составляющих
	1.2	Место информационной безопасности в системе национальной безопасности страны
	1.3	Источники угроз информационной безопасности и меры по их предотвращению
	1.4	Современные средства и способы обеспечения информационной безопасности
	1.5	Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи
Уметь	2.1	Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
	2.2	Классифицировать основные угрозы безопасности информации
	2.3	Применять основные правила и документы сертификации Российской Федерации

## 1.4. Формируемые компетенции:

ОК.1 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК.2 Организовывать собственную деятельность, выбирать типовые методы и

способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК.3 Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК.4 Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК.5 Использовать информационно-коммуникационные технологии в профессиональной деятельности.

**1.5. Рекомендуемое количество часов на освоение программы дисциплины:**

максимальный объем учебной нагрузки обучающегося 96 часа (ов), в том числе:

объем аудиторной учебной нагрузки обучающегося 64 часа (ов);

объем внеаудиторной работы обучающегося 32 часа (ов).

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 2.1. Объем дисциплины и виды учебной работы

<b>Виды учебной работы</b>	<b>Объем часов</b>
<b>Максимальный объем учебной нагрузки</b>	<b>96</b>
<b>Объем аудиторной учебной нагрузки</b>	<b>64</b>
в том числе:	
лабораторные работы	0
практические занятия	0
курсовая работа, курсовой проект	0
<b>Объем внеаудиторной работы обучающегося</b>	<b>32</b>
Промежуточная аттестация в форме "Дифференцированный зачет" (семестр 7)	

## 2.2. Тематический план и содержание дисциплины

Наименование разделов	Содержание учебного материала, теоретических занятий, практических занятий, лабораторных работ, самостоятельной работы обучающихся, курсовой работы, курсового проекта	Объём часов	№ дидактической единицы	Формируемые компетенции	Текущий контроль
1	2	4	5	6	7
<b>Раздел 1</b>	<b>Основы информационной безопасности</b>	<b>12</b>			
<b>Тема 1.1</b>	<b>Сущность и понятие информационной безопасности, характеристику ее составляющих</b>	<b>6</b>			
Занятие 1.1.1 теория	Введение в проблему информационной безопасности, ее актуальность	2	1.1	ОК.1	
Занятие 1.1.2 теория	Цели и задачи обеспечения информационной безопасности для различных объектов	2	1.1	ОК.1	
Занятие 1.1.3 теория	Основные составляющие информационной безопасности	2	1.1	ОК.1	
<b>Тема 1.2</b>	<b>Место информационной безопасности в системе национальной безопасности страны</b>	<b>6</b>			
Занятие 1.2.1 теория	Понятие национальной безопасности	2	1.2	ОК.5	
Занятие 1.2.2 теория	Обеспечение национальной безопасности Российской Федерации	2	1.2, 1.5, 2.3	ОК.4	
Занятие 1.2.3 теория	Информационная безопасность как состояние защищенности национальных интересов в информационной сфере	2	1.2, 2.3	ОК.2	1.1, 1.2, 2.3
<b>Раздел 2</b>	<b>Моделирование системы защиты информации</b>	<b>22</b>			
<b>Тема 2.1</b>	<b>Источники угроз информационной безопасности и меры по их предотвращению</b>	<b>22</b>			
Занятие 2.1.1 теория	Угрозы информационной безопасности Российской Федерации	2	1.3	ОК.1	

Занятие 2.1.2 теория	Принципы и приоритетные направления государственной политики обеспечения информационной безопасности	2	1.3	ОК.1	
Занятие 2.1.3 теория	Угрозы безопасности автоматизированных систем	2	1.3	ОК.1	
Занятие 2.1.4 теория	Меры и основные принципы обеспечения безопасности автоматизированных систем	2	1.3	ОК.2	
Занятие 2.1.5 теория	Анализ и оценка информационных рисков, угроз и уязвимостей системы	2	1.3, 2.2	ОК.5	
Занятие 2.1.6 теория	Проектирование системы защиты информации с использованием модели с полным перекрытием множества угроз	4	1.3, 2.2	ОК.3, ОК.5	
Занятие 2.1.7 теория	Анализ рисков информационной безопасности с использованием методики COBIT	4	1.3, 2.2	ОК.2, ОК.5	
Занятие 2.1.8 теория	Анализ рисков информационной безопасности для малого и среднего бизнеса	4	1.3, 2.2	ОК.2, ОК.3, ОК.5	1.3, 2.2
<b>Раздел 3</b>	<b>Системный подход к обеспечению информационной безопасности</b>	<b>30</b>			
<b>Тема 3.1</b>	<b>Современные средства и способы обеспечения информационной безопасности</b>	<b>20</b>			
Занятие 3.1.1 теория	Обеспечение информационной безопасности Российской Федерации	2	1.4	ОК.1	
Занятие 3.1.2 теория	Обеспечение безопасности автоматизированных систем	4	1.4	ОК.1	
Занятие 3.1.3 теория	Обеспечение безопасности компьютерных сетей	6	1.4	ОК.1	
Занятие 3.1.4 теория	Отечественные и зарубежные программно-технические средства защиты информации в интегрированных информационных системах управления предприятием	4	1.4	ОК.1	
Занятие 3.1.5	Вредоносные программы и защита от них	4	1.4	ОК.1	



теория					
<b>Тема 3.2</b>	<b>Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи</b>	<b>10</b>			
Занятие 3.2.1 теория	Концепция управления жизненным циклом конфиденциальной информации	4	1.5, 2.1	ОК.1, ОК.3	
Занятие 3.2.2 теория	Категорирование и документирование защищаемых ресурсов	4	1.5, 2.1	ОК.1, ОК.3, ОК.4	1.4, 1.5, 2.1
Занятие 3.2.3 теория	Дифференцированный зачет	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.2, ОК.5	
<b>Тематика самостоятельных работ</b>					
Номер по порядку	Вид (название) самостоятельной работы	Объем часов			
1	Поиск исторических фактов и событий нарушения информационной безопасности	2			
2	Составление глоссария "Информационная безопасность"	2			
3	Поиск документов	2			
4	Сопоставление различных точек зрения по теме "Обеспечение национальной безопасности РФ"	2			
5	Создание плакат-схемы "Угрозы информационной безопасности РФ"	2			
6	Создание плакат-схемы "Угрозы безопасности автоматизированных систем"	2			
7	Поиск информационных источников	3			
8	Составление отчета о работе "Использование методики COBIT"	3			
9	Составление отчета о работе "Анализ рисков для малого и среднего бизнеса"	2			
10	Систематизирование обязанностей пользователей и ответственных	2			

	за обеспечение информационной безопасности				
11	Разработка презентации "Средства защиты автоматизированных систем"	2			
12	Составление глоссария "Типовые удаленные атаки и их характеристики"	2			
13	Разработка презентации "Программно-технические средства защиты"	2			
14	Составление глоссария "Вредоносные программы"	2			
15	Построение схемы "Категорирование и документирование ресурсов"	2			
	ВСЕГО:	96			

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

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

Реализация программы дисциплины требует наличия учебного кабинета:  
Лаборатория информационно-коммуникационных систем.

#### 3.2. Информационное обеспечение обучения

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

№	Библиографическое описание	Тип (основной источник, дополнительный источник, электронный ресурс)
1.	Хорев П.Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. - М. : ФОРУМ, 2009. - 352 с.	[дополнительная]
2.	Васильков А.В. Информационные системы и их безопасность : учебное пособие / А.В. Васильков, А.А. Васильков, И.А.. Васильков. - М. : ФОРУМ, 2010. - 528 с.	[дополнительная]
3.	Васильков А.В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А.. Васильков. - М. : ФОРУМ, 2010. - 368 с.	[дополнительная]
4.	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие для СПО / В.Ф. Шаньгин. - М. : ФОРУМ, 2009. - 415 с.	[основная]

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

### 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
<b>Текущий контроль № 1.</b> <b>Методы и формы:</b> Письменный опрос (Опрос) <b>Вид контроля:</b> Проверочная работа	
1.1 Сущность и понятие информационной безопасности, характеристику ее составляющих	1.1.1, 1.1.2, 1.1.3
1.2 Место информационной безопасности в системе национальной безопасности страны	1.2.1, 1.2.2
2.3 Применять основные правила и документы сертификации Российской Федерации	1.2.2
<b>Текущий контроль № 2.</b> <b>Методы и формы:</b> Письменный опрос (Опрос) <b>Вид контроля:</b> Проверочная работа	
1.3 Источники угроз информационной безопасности и меры по их предотвращению	2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7
2.2 Классифицировать основные угрозы безопасности информации	2.1.5, 2.1.6, 2.1.7
<b>Текущий контроль № 3.</b> <b>Методы и формы:</b> Творческая работа (доклад, презентация) (Опрос) <b>Вид контроля:</b> Задание с применением ИКТ	
1.4 Современные средства и способы обеспечения информационной безопасности	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5
1.5 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	1.2.2, 3.2.1

2.1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	3.2.1
-----------------------------------------------------------------------------------------	-------

#### 4.2. Промежуточная аттестация

<b>№ семестра</b>	<b>Вид промежуточной аттестации</b>
7	Дифференцированный зачет

<b>Дифференцированный зачет может быть выставлен автоматически по результатам текущих контролей</b>
Текущий контроль №1
Текущий контроль №2
Текущий контроль №3

**Методы и формы:** Тестирование (Опрос)

**Описательная часть:** Ответьте на 24 вопроса теста

<b>Результаты обучения (освоенные умения, усвоенные знания)</b>	<b>Индекс темы занятия</b>
1.1 Сущность и понятие информационной безопасности, характеристику ее составляющих	1.1.1, 1.1.2, 1.1.3, 3.2.3
1.2 Место информационной безопасности в системе национальной безопасности страны	1.2.1, 1.2.2, 1.2.3, 3.2.3
1.3 Источники угроз информационной безопасности и меры по их предотвращению	2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.1.6, 2.1.7, 2.1.8, 3.2.3
1.4 Современные средства и способы обеспечения информационной безопасности	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.2.3
1.5 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	1.2.2, 3.2.1, 3.2.2, 3.2.3
2.1 Классифицировать защищаемую информацию по видам тайны и	3.2.1, 3.2.2, 3.2.3

степеням конфиденциальности	
2.2 Классифицировать основные угрозы безопасности информации	2.1.5, 2.1.6, 2.1.7, 2.1.8, 3.2.3
2.3 Применять основные правила и документы сертификации Российской Федерации	1.2.2, 1.2.3, 3.2.3

#### **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».