Министерство образования Иркутской области
Областное государственное образовательное учреждение среднего профессионального образования
«Иркутский авиационный техникум»

УТВЕРЖДАЮ
Директор
ОГБОУ СПО "ИАТ"

_____/Семёнов В.Г.
«30» мая 2014 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.12 Безопасность информационных систем

специальности

09.02.03 Программирование в компьютерных системах

Иркутск, 2014

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

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.12 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.5 Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК.9 Ориентироваться в условиях частой смены технологий 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

Виды учебной работы	Объем часов
Максимальный объем учебной нагрузки	**96**
Объем аудиторной учебной нагрузки	**64**
в том числе:	
лабораторные работы	0
практические занятия	0
курсовая работа, курсовой проект	0
Объем внеаудиторной работы обучающегося	**32**
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
Раздел 1	**Введение в информационную безопасность**	**22**			
Тема 1.1	**Сущность и понятие информационной безопасности**	**4**			
Занятие 1.1.1 теория	Основные понятия информационной безопасности.	2	1.1	ОК.1, ОК.2	
Занятие 1.1.2 теория	Анализ угроз информационной безопасности	2	1.1	ОК.1, ОК.2	
Тема 1.2	**Информационная безопасность РФ**	**10**			
Занятие 1.2.1 теория	Информационная безопасность в системе национальной безопасности Российской Федерации	2	1.2, 2.3	ОК.1, ОК.2,	
Занятие 1.2.2 теория	Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.	2	1.2	ОК.1, ОК.2,	
Занятие 1.2.3 теория	Основные положения государственной информационной политики России	2	1.2, 2.3	ОК.1, ОК.2,	
Занятие 1.2.4 теория	Доктрина информационной безопасности Российской Федерации	2	1.2, 2.3	ОК.1, ОК.2,	
Занятие 1.2.5 теория	Анализ Доктрины информационной безопасности Российской Федерации	2	2.1, 2.2	ОК.2, ОК.5, ОК.9	
Тема 1.3	**Разновидности атак на защищаемые ресурсы**	**8**			
Занятие 1.3.1 теория	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации	2	1.3	ОК.2, ОК.5, ОК.9	
Занятие 1.3.2 теория	Методы оценки уязвимости информации. Виды утечки информации.	2	1.3	ОК.2, ОК.5, ОК.9	

Занятие 1.3.3 теория	Информация как объект защиты	2	1.1, 1.3	ОК.2, ОК.5	
Занятие 1.3.4 теория	Итоговое занятие по теме "Введение в информационную безопасность"	2	1.1, 1.2, 1.3	ОК.2, ОК.5	1.1, 1.2, 1.3
Раздел 2	**Источники и носители защищаемой информации**	**10**			
Тема 2.1	**Конфиденциальная информация**	**10**			
Занятие 2.1.1 теория	Понятие конфиденциальной информации.	2	1.5	ОК.2, ОК.9	
Занятие 2.1.2 теория	Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.	2	1.5	ОК.2	
Занятие 2.1.3 теория	Жизненные циклы конфиденциальной информации	2	1.5	ОК.2, ОК.9	
Занятие 2.1.4 теория	Защита информации составляющей государственную тайну	2	1.5	ОК.2, ОК.5	
Занятие 2.1.5 теория	Защита информации, охраняемая авторским и патентным правом.	2	1.5	ОК.2	
Раздел 3	**Средства и способы обеспечения информационной безопасности**	**32**			
Тема 3.1	**Защита от несанкционированного доступа, модели и основные принципы защиты информации**	**14**			
Занятие 3.1.1 теория	Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД)	2	1.4	ОК.2, ОК.5, ОК.9	
Занятие 3.1.2 теория	Стандарты в области информационной безопасности АСОД	2	1.4	ОК.2, ОК.5, ОК.9	
Занятие 3.1.3 теория	Показатели защищенности СВТ. Защита информации в АСОД	2	1.4	ОК.2, ОК.5, ОК.9	
Занятие 3.1.4 теория	Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа	2	1.4	ОК.2, ОК.5	

Занятие 3.1.5 теория	Автоматизированная система, как объект информационной защиты.	2	1.4	ОК.2, ОК.5	
Занятие 3.1.6 теория	Основные методы и приемы защиты от несанкционированного доступа	2	1.4	ОК.2, ОК.5	
Занятие 3.1.7 теория	Средства и способы обеспечения информационной безопасности	2	1.4	ОК.2, ОК.5	1.4, 1.5
Тема 3.2	**Компьютерные вирусы и антивирусные программы**	**4**			
Занятие 3.2.1 теория	Проблема вирусного заражения программ. Классификация вирусов. Способы заражения программ	2	1.4	ОК.2, ОК.5	
Занятие 3.2.2 теория	Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ	2	1.4	ОК.2, ОК.5	
Тема 3.3	**Технология обнаружения вторжения**	**14**			
Занятие 3.3.1 теория	Адаптивное управление безопасностью	2	1.4	ОК.2, ОК.5	
Занятие 3.3.2 теория	Средства анализа защищенности сетевых протоколов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности	2	1.4	ОК.2, ОК.5	
Занятие 3.3.3 теория	Методы анализа сетевой информации	2	1.4	ОК.2, ОК.5	
Занятие 3.3.4 теория	Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей	2	1.4	ОК.2, ОК.5	
Занятие 3.3.5 теория	Основы сетевого и межсетевого взаимодействия	2	1.4	ОК.2, ОК.5	
Занятие 3.3.6 теория	Технологии межсетевых экранов. Требования и показатели защищенности межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов	2	1.4	ОК.2, ОК.5	
Занятие 3.3.7	Политика безопасности. Сетевая политика безопасности	2	1.4	ОК.2, ОК.5	2.1, 2.2, 2.3

теория					
Тематика самостоятельных работ					
Номер по порядку	Вид (название) самостоятельной работы	Объем часов			
1	Конспект по теме криптология. Этапы развития. Стеганография.	1			
2	Конспект по теме криптология. Этапы развития. Стеганография	1			
3	Конспект по теме шифрование заменой (подстановка). Шифр Цезаря. Шифр Атбаш	1			
4	Конспект по теме шифрование заменой (подстановка). Шифр Цезаря. Шифр Атбаш	1			
5	Конспект по теме квадрат Полибия	1			
6	Конспект по теме квадрат Полибия	1			
7	Конспект по теме афинные криптосистемы	1			
8	Конспект по теме афинные криптосистемы	1			
9	Конспект по теме моноалфавитная подстановка	1			
10	Конспект по теме моноалфавитная подстановка	1			
11	Конспект по теме полиалфавитная подстановка	1			
12	Конспект по теме полиалфавитная подстановка	1			
13	Конспект по теме таблица Вижинера	1			
14	Конспект по теме таблица Вижинера	1			
15	Конспект по теме квадрат Бьюфорта	1			
16	Конспект по теме квадрат Бьюфорта	1			
17	Конспект по теме монофоническая замена	1			
18	Конспект по теме монофоническая замена	1			
19	Конспект по теме полиалфавитная подстановка	1			
20	Конспект по теме полиалфавитная подстановка	1			

21	Конспект по теме система Плейфера	1			
22	Конспект по теме система Плейфера	1			
23	Конспект по теме шифрование методом перестановки	1			
24	Конспект по теме шифрование с помощью аналитических преобразований	1			
25	Конспект по теме шифрование с помощью аналитических преобразований	1			
26	Конспект по теме шифрование методом гаммирования	1			
27	Конспект по теме шифрование методом гаммирования	1			
28	Конспект по теме система с открытым ключом	1			
29	Конспект по теме система с открытым ключом	1			
30	Конспект по теме система с открытым ключом	1			
31	Конспект по теме Электронно-цифровая подпись	1			
32	Конспект по теме Электронно-цифровая подпись	1			
	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.	Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие для СПО / В.Ф. Шаньгин. - М. : ФОРУМ, 2009. - 415 с.	[основная]
2.	Васильков А.В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А.. Васильков. - М. : ФОРУМ, 2010. - 368 с.	[дополнительная]
3.	Хорев П.Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. - М. : ФОРУМ, 2009. - 352 с.	[дополнительная]
4.	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]

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
Текущий контроль № 1. **Методы и формы:** Тестирование (Опрос) **Вид контроля:** письменное тестирование	
1.1 Сущность и понятие информационной безопасности, характеристику ее составляющих	1.1.1, 1.1.2, 1.3.3
1.2 Место информационной безопасности в системе национальной безопасности страны	1.2.1, 1.2.2, 1.2.3, 1.2.4
1.3 Источники угроз информационной безопасности и меры по их предотвращению	1.3.1, 1.3.2, 1.3.3
Текущий контроль № 2. **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** проверочная работа	
1.4 Современные средства и способы обеспечения информационной безопасности	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6
1.5 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5
Текущий контроль № 3. **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Проверочная работа	
2.1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	1.2.5
2.2 Классифицировать основные угрозы безопасности информации	1.2.5

2.3 Применять основные правила и документы сертификации Российской Федерации	1.2.1, 1.2.3, 1.2.4

4.2. Промежуточная аттестация

№ семестра	Вид промежуточной аттестации
7	Дифференцированный зачет

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

Методы и формы: Контрольная работа (Опрос)
Описательная часть: по выбору выполнить два теоретических задания

Результаты обучения (освоенные умения, усвоенные знания)	Индекс темы занятия
1.1 Сущность и понятие информационной безопасности, характеристику ее составляющих	1.1.1, 1.1.2, 1.3.3, 1.3.4
1.2 Место информационной безопасности в системе национальной безопасности страны	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.3.4
1.3 Источники угроз информационной безопасности и меры по их предотвращению	1.3.1, 1.3.2, 1.3.3, 1.3.4
1.4 Современные средства и способы обеспечения информационной безопасности	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 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, 3.3.7
1.5 Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи	2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5
2.1 Классифицировать защищаемую информацию по видам тайны и	1.2.5

степеням конфиденциальности	
2.2 Классифицировать основные угрозы безопасности информации	1.2.5
2.3 Применять основные правила и документы сертификации Российской Федерации	1.2.1, 1.2.3, 1.2.4

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».