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

УТВЕРЖДАЮ
и.о. директора
ГБПОУИО «ИАТ»
_____/Коробкова Е.А.
«31» мая 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.14 Безопасность информационных систем

специальности

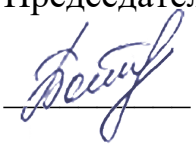
09.02.01 Компьютерные системы и комплексы

Иркутск, 2019

Рассмотрена
цикловой комиссией
КС протокол №9 от 28.03.2019 г.

Рабочая программа разработана на основе ФГОС СПО специальности 09.02.01 Компьютерные системы и комплексы; учебного плана специальности 09.02.01 Компьютерные системы и комплексы; на основе рекомендаций работодателя (протокол заседания ВЦК КС №8 от 06.03.2019 г.).

Председатель ЦК


_____ /М.А. Богачева /

№	Разработчик ФИО
1	Шатурский Дмитрий Витальевич

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	14

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.14 БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

1.1. Область применения рабочей программы (РП)

РП является частью программы подготовки специалистов среднего звена по специальности 09.02.01 Компьютерные системы и комплексы.

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.
ОК.6 Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК.7 Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.
ОК.8 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
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 114 часа (ов), в том числе:
объем аудиторной учебной нагрузки обучающегося 76 часа (ов);
объем внеаудиторной работы обучающегося 38 часа (ов).

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Виды учебной работы	Объем часов
Максимальный объем учебной нагрузки	**114**
Объем аудиторной учебной нагрузки	**76**
в том числе:	
лабораторные работы	0
практические занятия	16
курсовая работа, курсовой проект	0
Объем внеаудиторной работы обучающегося	**38**
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, 2.2	ОК.1, ОК.3, ОК.5	
Занятие 1.1.2 теория	Анализ угроз информационной безопасности	2	1.1, 1.2, 2.2	ОК.1, ОК.3, ОК.5	
Тема 1.2	**Информационная безопасность РФ**	**10**			
Занятие 1.2.1 теория	Информационная безопасность в системе национальной безопасности Российской Федерации	2	1.2, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	
Занятие 1.2.2 теория	Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	
Занятие 1.2.3 теория	Основные положения государственной информационной политики России	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.9	
Занятие 1.2.4 теория	Доктрина информационной безопасности Российской Федерации	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5	
Занятие 1.2.5 практическое занятие	Анализ Доктрины информационной безопасности Российской Федерации	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5	
Тема 1.3	**Разновидности атак на защищаемые ресурсы**	**8**			
Занятие 1.3.1 теория	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5	
Занятие 1.3.2	Методы оценки уязвимости информации. Виды утечки	2	1.1, 1.2, 1.3, 1.4,	ОК.1, ОК.3, ОК.5	

теория	информации.		1.5, 2.1, 2.2, 2.3		
Занятие 1.3.3 практическое занятие	Информация как объект защиты	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	
Занятие 1.3.4 практическое занятие	Итоговое занятие по теме "Введение в информационную безопасность"	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	1.1, 1.2, 2.1
Раздел 2	**Источники и носители защищаемой информации**	**10**			
Тема 2.1	**Конфиденциальная информация**	**10**			
Занятие 2.1.1 теория	Понятие конфиденциальной информации.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3	
Занятие 2.1.2 теория	Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3	
Занятие 2.1.3 теория	Жизненные циклы конфиденциальной информации	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	
Занятие 2.1.4 теория	Защита информации составляющей государственную тайну	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	
Занятие 2.1.5 теория	Защита информации, охраняемая авторским и патентным правом.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	
Раздел 3	**Средства и способы обеспечения информационной безопасности**	**44**			
Тема 3.1	**Защита от несанкционированного доступа, модели и основные принципы защиты информации**	**16**			
Занятие 3.1.1 теория	Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД)	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	
Занятие 3.1.2 теория	Стандарты в области информационной безопасности АСОД	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.8	
Занятие 3.1.3	Показатели защищенности СВТ. Защита информации в АСОД	2	1.1, 1.2, 1.3, 1.4,	ОК.2, ОК.3, ОК.6	

теория			1.5, 2.1, 2.2, 2.3		
Занятие 3.1.4 теория	Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.4, ОК.6	
Занятие 3.1.5 теория	Автоматизированная система, как объект информационной защиты.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.4	
Занятие 3.1.6 теория	Основные методы и приемы защиты от несанкционированного доступа	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.5, ОК.7	
Занятие 3.1.7 практическое занятие	Методы и средства защиты информации	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.5, ОК.6, ОК.7, ОК.8, ОК.9	
Занятие 3.1.8 практическое занятие	Средства и способы обеспечения информационной безопасности	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.7	1.3, 1.4, 2.2
Тема 3.2	**Компьютерные вирусы и антивирусные программы**	**4**			
Занятие 3.2.1 теория	Проблема вирусного заражения программ. Классификация вирусов. Способы заражения программ	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.5, ОК.9	
Занятие 3.2.2 теория	Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.5, ОК.9	
Тема 3.3	**Технология обнаружения вторжения**	**24**			
Занятие 3.3.1 теория	Адаптивное управление безопасностью	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.5, ОК.9	
Занятие 3.3.2 теория	Средства анализа защищенности сетевых протоколов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.5, ОК.9	
Занятие 3.3.3 теория	Методы анализа сетевой информации	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3, ОК.5, ОК.9	
Занятие 3.3.4	Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных	2	1.1, 1.2, 1.3, 1.4,	ОК.3, ОК.5, ОК.9	

теория	корпоративных сетей. Угрозы и уязвимости беспроводных сетей		1.5, 2.1, 2.2, 2.3		
Занятие 3.3.5 теория	Основы сетевого и межсетевого взаимодействия	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.5, ОК.9	
Занятие 3.3.6 теория	Технологии межсетевых экранов. Требования и показатели защищенности межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.4, ОК.9	
Занятие 3.3.7 теория	Политика безопасности. Сетевая политика безопасности	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.7, ОК.9	
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.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.6	
Занятие 3.3.9 теория	Обзор современных средств обнаружения атак	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.9	
Занятие 3.3.10 практическое занятие	Анализ защищенности объекта защиты информации	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.3, ОК.5, ОК.7	1.4, 1.5, 2.3
Занятие 3.3.11 практическое занятие	Построение модели потенциального нарушителя информационной системы	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.3	
Занятие 3.3.12 практическое занятие	Итоговое занятие	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.2, ОК.3,	
Тематика самостоятельных работ					
Номер по порядку	Вид (название) самостоятельной работы	Объем часов			
1	Написание конспекта по теме "Криптология. Этапы развития. Стеганография"	1			

2	Написание конспекта по теме "Криптология. Этапы развития. Стеганография"	1			
3	Написание конспекта по теме "Шифрование заменой (подстановка). Шифр Цезаря. Шифр Атбаш"	1			
4	Написание конспекта по теме "Шифрование заменой (подстановка). Шифр Цезаря. Шифр Атбаш"	1			
5	Написание конспекта по теме "Квадрат Полибия"	1			
6	Написание конспекта по теме "Квадрат Полибия"	1			
7	Написание конспекта по теме "Афинные криптосистемы"	1			
8	Написание конспекта по теме "Афинные криптосистемы"	1			
9	Написание конспекта по теме "Моноалфавитная подстановка"	1			
10	Написание конспекта по теме "Моноалфавитная подстановка"	1			
11	Написание конспекта по теме "Полиалфавитная подстановка"	1			
12	Написание конспекта по теме "Полиалфавитная подстановка"	1			
13	Написание конспекта по теме "Полиалфавитная подстановка"	1			
14	Написание конспекта по теме "Полиалфавитная подстановка"	1			
15	Написание конспекта по теме "Таблица Вижинера"	1			
16	Написание конспекта по теме "Таблица Вижинера"	1			
17	Написание конспекта по теме "Квадрат Бьюфорта"	1			
18	Написание конспекта по теме "Квадрат Бьюфорта"	1			
19	Написание конспекта "Монофоническая замена"	1			
20	Написание конспекта "Монофоническая замена"	1			
21	Написание конспекта по теме "Система Плейфера"	1			
22	Написание конспекта по теме "Система Плейфера"	1			
23	Написание конспекта по теме "Шифрование методом перестановки"	1			

24	Написание конспекта по теме "Шифрование методом перестановки"	1			
25	Написание конспекта по теме "Шифрование с помощью аналитических преобразований"	1			
26	Написание конспекта по теме "Шифрование с помощью аналитических преобразований"	1			
27	Написание конспекта по теме "Шифрование методом гаммирования"	1			
28	Написание конспекта по теме "Шифрование методом гаммирования"	1			
29	Написание конспекта по теме "Система с открытым ключом"	1			
30	Написание конспекта по теме "Система с открытым ключом"	1			
31	Написание конспекта по теме "Система с открытым ключом"	1			
32	Написание конспекта по теме "Электронно-цифровая подпись"	1			
33	Написание конспекта по теме "Электронно-цифровая подпись"	1			
34	Написание конспекта по теме "Электронно-цифровая подпись"	1			
35	Написание конспекта по теме "Электронно-цифровая подпись"	1			
36	Написание конспекта по теме "Информационная война. Информационное оружие."	1			
37	Написание конспекта по теме "Информационная война. Информационное оружие."	2			
	ВСЕГО:	114			

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета: Лаборатория интернет-технологий.

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)

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:** Письменный опрос (Опрос) **Вид контроля:** Проверочная работа	
1.1 сущность и понятие информационной безопасности, характеристику ее составляющих;	1.1.1, 1.1.2, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3
1.2 место информационной безопасности в системе национальной безопасности страны;	1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3
2.1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 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;	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7
1.3 источники угроз информационной безопасности и меры по их предотвращению;	1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7
2.2 классифицировать основные угрозы безопасности информации;	1.1.1, 1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7
Текущий контроль № 3. **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Проверочная работа	
1.4 современные средства и способы обеспечения информационной безопасности;	3.1.8, 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, 3.3.8, 3.3.9

1.5 жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9
2.3 применять основные правила и документы сертификации Российской Федерации.	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9

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: Письменный опрос (Опрос)
Описательная часть: по выбору выполнить одно теоретическое задание и одно практическое задание

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, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12
1.2 место информационной безопасности в системе национальной безопасности страны;	1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9,

	3.3.10, 3.3.11, 3.3.12
1.3 источники угроз информационной безопасности и меры по их предотвращению;	1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12
1.4 современные средства и способы обеспечения информационной безопасности;	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12
1.5 жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12
2.1 классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12
2.2 классифицировать основные угрозы безопасности информации;	1.1.1, 1.1.2, 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12
2.3 применять основные правила и документы сертификации Российской Федерации.	1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, 3.1.8, 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, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12

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».