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

УТВЕРЖДАЮ
Директор
ГБПОУИО «ИАТ»
_____ Якубовский А.Н.
«30» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП.15 Безопасность компьютерных систем

специальности

09.02.01 Компьютерные системы и комплексы

Иркутск, 2024

Рассмотрена
цикловой комиссией
КС протокол №5 от 07.02.2023 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 №3 от 15.11.2022 г.).

№	Разработчик ФИО
1	Тирский Андрей Ильич

СОДЕРЖАНИЕ

		стр.
1	ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	4
2	СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	7
3	УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	16
4	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	21

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОП.15 БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ 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:

Результаты освоения дисциплины	№ результата	Формируемый результат
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

Личностные результаты реализации программы воспитания	3.1	Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном и многоконфессиональном российском обществе, и современном мировом сообществе. Сознающий свое единство с народом России, с Российским государством, демонстрирующий ответственность за развитие страны. Проявляющий готовность к защите Родины, способный аргументированно отстаивать суверенитет и достоинство народа России, сохранять и защищать историческую правду о Российском государстве
	3.2	Проявляющий и демонстрирующий уважение законных интересов и прав представителей различных этнокультурных, социальных, конфессиональных групп в российском обществе; национального достоинства, религиозных убеждений с учётом соблюдения необходимости обеспечения конституционных прав и свобод граждан. Понимающий и деятельно выражающий ценность межрелигиозного и межнационального согласия людей, граждан, народов в России. Выражающий сопричастность к преумножению и трансляции культурных традиций и ценностей многонационального российского государства, включенный в общественные инициативы, направленные на их сохранение
	3.3	Сознающий ценность жизни, здоровья и безопасности. Соблюдающий и пропагандирующий здоровый образ жизни (здоровое питание, соблюдение гигиены, режим занятий и отдыха, физическая активность), демонстрирующий стремление к физическому совершенствованию. Проявляющий сознательное и обоснованное неприятие вредных привычек и опасных наклонностей (курение, употребление алкоголя, наркотиков, психоактивных веществ, азартных игр, любых форм зависимостей), деструктивного поведения в обществе, в том числе в цифровой среде

	3.4	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации

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.6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК.9 Пользоваться профессиональной документацией на государственном и иностранном языках
ПК.1.3 Оформлять техническую документацию на проектируемые устройства
ПК.3.1 Проводить контроль параметров, диагностику и восстановление работоспособности цифровых устройств компьютерных систем и комплексов

1.5. Количество часов на освоение программы дисциплины:
Общий объем дисциплины 88 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Виды учебной работы	Объем часов
Общий объем дисциплины	**88**
Работа обучающихся во взаимодействии с преподавателем:	**86**
теоретическое обучение	38
лабораторные занятия	0
практические занятия	42
Промежуточная аттестация в форме "Экзамен" (семестр 7)	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	**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, ПК.1.3	
Занятие 1.1.2 теория	Анализ угроз информационной безопасности.	2	1.1, 1.2, 2.2	ОК.3, ПК.1.3	
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.6, ПК.1.3	
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.6, ОК.9, ПК.1.3	
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	ПК.3.1	
Занятие 1.2.4 практическое занятие	Доктрина информационной безопасности Российской Федерации.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ПК.1.3	

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.3, ПК.1.3	
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.9, ПК.3.1	
Занятие 1.3.2 практическое занятие	Методы оценки уязвимости информации. Виды утечки информации.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.3, ПК.1.3, ПК.3.1	
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.2, ПК.1.3	
Занятие 1.3.4 практическое занятие	Объекты защиты информации.	1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ПК.1.3	1.1, 1.2, 2.1
Занятие 1.3.5 практическое занятие	Объекты защиты информации.	1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ПК.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	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.3, ПК.1.3	
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, ПК.1.3	
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.3, ОК.9, ПК.3.1	
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.2, ПК.3.1	

Занятие 2.1.5 практическое занятие	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.6, ПК.1.3	
Раздел 3	**Средства и способы обеспечения информационной безопасности**	**50**			
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, ПК.3.1	
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.2, ПК.1.3	
Занятие 3.1.3 теория	Показатели защищенности СВТ. Защита информации в АСОД.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.3, ОК.6, ПК.1.3	
Занятие 3.1.4 практическое занятие	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.3, ОК.6, ПК.1.3	
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.1, ОК.2, ПК.3.1	
Занятие 3.1.6 практическое занятие	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.1, ОК.2, ПК.1.3	
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.6, ОК.9, ПК.3.1	
Занятие 3.1.8 практическое занятие	Средства и способы обеспечения информационной безопасности.	1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.6, ПК.1.3	1.3, 1.4, 2.2

Занятие 3.1.9 практическое занятие	Средства и способы обеспечения информационной безопасности.	1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.6, ПК.1.3	
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.2, ОК.3, ПК.3.1	
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, 3.3	ОК.2, ОК.3, ПК.3.1	
Тема 3.3	**Технология обнаружения вторжения**	**30**			
Занятие 3.3.1 практическое занятие	Адаптивное управление безопасностью.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.2, ПК.3.1	
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.6, ПК.1.3, ПК.3.1	
Занятие 3.3.3 практическое занятие	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, ПК.1.3	
Занятие 3.3.4 теория	Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.2, ОК.6, ПК.3.1	
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.1, ОК.2, ОК.6, ПК.1.3	
Занятие 3.3.6 практическое занятие	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.1, ОК.6, ПК.3.1	
Занятие 3.3.7 практическое занятие	Политика безопасности. Сетевая политика безопасности.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, 3.4	ОК.1, ОК.6, ОК.9, ПК.1.3	

Занятие 3.3.8 практическое занятие	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.1, ОК.2, ПК.3.1	
Занятие 3.3.9 Самостоятельная работа	Обзор современных средств обнаружения атак.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.2, ПК.1.3	
Занятие 3.3.10 практическое занятие	Анализ защищенности объекта защиты информации.	1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.2, ПК.1.3	1.4, 1.5, 2.3
Занятие 3.3.11 практическое занятие	Анализ защищенности объекта защиты информации.	1	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3	ОК.1, ОК.2, ПК.1.3	
Занятие 3.3.12 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.2, ОК.3, ОК.9, ПК.1.3, ПК.3.1	
Занятие 3.3.13 практическое занятие	Разработка и декодирование сообщения с использованием шифра Виженера.	2	1.1, 1.2, 1.3, 1.4, 1.5, 2.1, 2.2, 2.3, 3.1, 3.2	ОК.2, ОК.9	
Занятие 3.3.14 практическое занятие	Исследование работы и принципов шифрования машины "Энигма".	2	1.2, 1.3, 2.1	ОК.3, ОК.6, ПК.1.3	
Занятие 3.3.15 практическое занятие	Принцип шифрования публичным ключом.	2	1.1, 1.4, 2.1, 2.2	ОК.1, ОК.3, ПК.1.3	
Занятие 3.3.16 практическое занятие	Шифр Вернама (XOR-шифр).	2	1.1, 1.2	ОК.1, ОК.3, ПК.3.1	
	Экзамен	6			

ВСЕГО:	88			

2.3. Формирование личностных результатов реализации программы воспитания

Наименование темы занятия	Наименование личностного результата реализации программы воспитания	Тип мероприятия	Наименование мероприятия
3.2.2 Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ	3.3 Сознающий ценность жизни, здоровья и безопасности. Соблюдающий и пропагандирующий здоровый образ жизни (здоровое питание, соблюдение гигиены, режим занятий и отдыха, физическая активность), демонстрирующий стремление к физическому совершенствованию. Проявляющий сознательное и обоснованное неприятие вредных привычек и опасных наклонностей (курение, употребление алкоголя, наркотиков, психоактивных веществ, азартных игр, любых форм зависимостей), деструктивного поведения в обществе, в том числе в цифровой среде	Беседа	Вирусные программы.

3.3.7 Политика безопасности. Сетевая политика безопасности.	3.4 Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации	Диспут	Политика безопасности.
3.3.13 Разработка и декодирование сообщения с использованием шифра Виженера.	3.1 Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном и многоконфессиональном российском обществе, и современном мировом сообществе. Сознающий свое единство с народом России, с Российским государством, демонстрирующий ответственность за развитие страны. Проявляющий готовность к защите Родины, способный аргументированно отстаивать суверенитет и достоинство народа России, сохранять и защищать историческую правду о Российском государстве	Круглый стол	Шифры

3.3.13 Разработка и декодирование сообщения с использованием шифра Виженера.	3.2 Проявляющий и демонстрирующий уважение законных интересов и прав представителей различных этнокультурных, социальных, конфессиональных групп в российском обществе; национального достоинства, религиозных убеждений с учётом соблюдения необходимости обеспечения конституционных прав и свобод граждан. Понимающий и деятельно выражающий ценность межрелигиозного и межнационального согласия людей, граждан, народов в России. Выражающий сопричастность к преумножению и трансляции культурных традиций и ценностей многонационального российского государства, включенный в общественные инициативы, направленные на их сохранение	Беседа	Декодирование шифров

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета: Лаборатория информационных технологий.

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

Наименование занятия ЛПР	**Перечень оборудования**
1.1.1 Основные понятия информационной безопасности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.1.2 Анализ угроз информационной безопасности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.2.1 Информационная безопасность в системе национальной безопасности Российской Федерации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.2.2 Сущность и понятие информационной безопасности. Принципы обеспечения информационной безопасности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.2.3 Основные положения государственной информационной политики России.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.2.4 Доктрина информационной безопасности Российской Федерации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.2.5 Анализ Доктрины информационной безопасности Российской Федерации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.3.1 Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.3.2 Методы оценки уязвимости информации. Виды утечки информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор

1.3.3 Информация как объект защиты.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.3.4 Объекты защиты информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
1.3.5 Объекты защиты информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
2.1.1 Понятие конфиденциальной информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
2.1.2 Классификация конфиденциальной информации по видам тайны и степени конфиденциальности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
2.1.3 Жизненные циклы конфиденциальной информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
2.1.4 Защита информации составляющей государственную тайну.	Microsoft Windows 7, Персональный компьютер, Google Chrome, OpenOffice, Плазменный телевизор
2.1.5 Защита информации, охраняемая авторским и патентным правом.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.1 Интегральная безопасность. Угрозы безопасности автоматизированных систем обработки данных (АСОД).	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.2 Стандарты в области информационной безопасности АСОД.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.3 Показатели защищенности СВТ. Защита информации в АСОД.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.4 Методы и системы защиты информации. Виды доступа. Уровни доступа. Контроль доступа.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор

3.1.5 Автоматизированная система, как объект информационной защиты.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.6 Основные методы и приемы защиты от несанкционированного доступа.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.7 Методы и средства защиты информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.8 Средства и способы обеспечения информационной безопасности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.1.9 Средства и способы обеспечения информационной безопасности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.2.1 Проблема вирусного заражения программ. Классификация вирусов. Способы заражения программ.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.2.2 Структура современных вирусных программ. Перспективные методы антивирусной защиты. Основные классы антивирусных программ	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.1 Адаптивное управление безопасностью.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.2 Средства анализа защищенности сетевых протоколов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.3 Методы анализа сетевой информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.4 Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор

3.3.5 Основы сетевого и межсетевого взаимодействия.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.6 Технологии межсетевых экранов. Требования и показатели защищенности межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.7 Политика безопасности. Сетевая политика безопасности.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.8 Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности обнаружения атак на сетевом и операционном уровне. Реагирование на атаку.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.9 Обзор современных средств обнаружения атак.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.10 Анализ защищенности объекта защиты информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.11 Анализ защищенности объекта защиты информации.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.12 Построение модели потенциального нарушителя информационной системы.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.13 Разработка и декодирование сообщения с использованием шифра Виженера.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.14 Исследование работы и принципов шифрования машины "Энигма".	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор
3.3.15 Принцип шифрования публичным ключом.	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор

3.3.16 Шифр Вернама (XOR-шифр).	Microsoft Windows 7, Персональный компьютер, Google Chrome, Microsoft Office 2010, Плазменный телевизор

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)
1.	Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/145912.html — Режим доступа: для авторизир. пользователей	[основная]
2.	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

Контроль и оценка результатов освоения дисциплины проводится на основе заданий и критериев их оценивания, представленных в фондах оценочных средств по дисциплине ОП.15 Безопасность компьютерных 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 (40 минут). **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 (30 минут). **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, 1.3.5, 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, 1.3.5, 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, 1.3.5, 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 (30 минут). **Методы и формы:** Письменный опрос (Опрос) **Вид контроля:** Проверочная работа	
1.4 современные средства и способы обеспечения информационной безопасности	3.1.8, 3.1.9, 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, 1.3.5, 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, 3.1.9, 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, 1.3.5, 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, 3.1.9, 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	Экзамен

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

Методы и формы: Практическая работа (Опрос)
Описательная часть: По выбору выполнить 1 теоретическое задание и 1 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, 1.3.5, 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, 3.1.9, 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, 3.3.13, 3.3.15, 3.3.16
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, 1.3.5, 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, 3.1.9, 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, 3.3.13, 3.3.14, 3.3.16
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, 1.3.5, 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, 3.1.9, 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, 3.3.13, 3.3.15
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, 1.3.5, 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, 3.1.9, 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, 3.3.13, 3.3.14
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, 1.3.5, 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, 3.1.9, 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, 3.3.13
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, 1.3.5, 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, 3.1.9, 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, 3.3.13, 3.3.15

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, 1.3.5, 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, 3.1.9, 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, 3.3.13
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, 1.3.5, 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, 3.1.9, 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, 3.3.13, 3.3.14, 3.3.15

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».