Бюджетное учреждение высшего образования
Ханты-Мансийского автономного округа-Югры
"Сургутский государственный университет"

УТВЕРЖДАЮ
Проректор по УМР

_____Е.В. Коновалова

13 июня 2024г., протокол УМС №5

Риски и безопасность

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Автоматизированных систем обработки информации и управления**

Учебный план g090401-ИнфПрогОб-24-2.plx
09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Информационное и программное обеспечение автоматизированных систем

Квалификация **Магистр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 32
самостоятельная работа 31
часов на контроль 45

Виды контроля в семестрах:
экзамены 3

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**3 (2.1)**		Итого	
Недель	17 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	31	31	31	31
Часы на контроль	45	45	45	45
Итого	108	108	108	108

Программу составил(и):
к.т.н., Доцент, Гавриленко Т.В.

Рабочая программа дисциплины
Риски и безопасность

разработана в соответствии с ФГОС:
Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

составлена на основании учебного плана:
09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Информационное и программное обеспечение автоматизированных систем
утвержденного учебно-методическим советом вуза от 13.06.2024 протокол № 5.

Рабочая программа одобрена на заседании кафедры
Автоматизированных систем обработки информации и управления

Зав. кафедрой Доцент кафедры АСОИУ, к.т.н., Бушмелева К.И.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Сформировать знаний об основных положениях теории и практики информационной безопасности.
1.2	Сформировать умения применять современные методы и средства защиты информации в вычислительных системах и сетях.
1.3	Сформировать компетенции в области разработки и использования средств защиты компьютерной информации в процессе ее обработки, передачи и хранения в информационных системах.
1.4	Сформировать способность разрабатывать оригинальные алгоритмы и программные средства с учётом рисков и требований информационной безопасности.
1.5	Сформировать способность применения на практике новых подходов и методов к исследованию рисков информационной безопасности.
1.6	Сформировать способность учитывать риски информационной безопасности при разработке компонентов программно-аппаратных комплексов обработки информации и автоматизированного проектирования.
1.7	Сформировать способность экспертного анализа эргономических характеристик программных продуктов с учетом рисков связанных с нарушением информационной безопасности пользователем обладающим низкой квалификацией.
1.8	Сформировать способность оценивать риски при интеграции системного программного обеспечения.
1.9	Сформировать способность при разработке комплексных проектов учитывать риски информационной безопасности.
1.10	Сформировать способность управления программно-техническими, технологическими и человеческими ресурсами с учетом рисков и информационной безопасности.
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Математическое моделирование объектов и систем управления
2.1.2	Системный анализ и управление информацией
2.1.3	История и методология информатики и вычислительной техники
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика, проектно-технологическая практика
2.2.2	Производственная практика, преддипломная практика
2.2.3	Выполнение и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-1.1: Демонстрирует знания архитектуры, устройства и функционирования вычислительных систем. Возможностей ИС. Инструментов и методов: модульного тестирования; тестирования нефункциональных и функциональных характеристик ИС; физического и функционального аудита конфигурации ИС. Источников информации, необходимых для профессиональной деятельности. Ключевых возможностей ИС. Коммуникационного оборудования. Конфигурационного управления. Программных средств и платформ инфраструктуры информационных технологий организаций. Регламентов развертывания ИС. Сетевых протоколов. Современных методик тестирования разрабатываемых ИС. Современных стандартов информационного взаимодействия систем. Управления качеством: контрольные списки, верификация, валидация (приемо-сдаточные испытания). Устройства и функционирования современных ИС

ПК-1.2: Анализирует исходную документацию. Выполняет аудит конфигураций ИС. Проверяет (верифицировать) архитектуру и дизайн ИС. Проводит аудит качества в проектах. Производит приемо-сдаточные испытания. Составляет отчетность.

ПК-1.3: Владеет навыками внедрения инструментов и методов контроля качества. Выбора и разработки инструментов и методов идентификации конфигурации. Обеспечения соответствия проектирования и дизайна ИС, процессов идентификации конфигурации ИС, принятым в организации или проекте стандартам и технологиям. Определения базовых элементов конфигурации ИС. Интервьюирования представителей заказчика и подписания документов по результатам приемо-сдаточных испытаний. Экспертной поддержки инициирования работ по реализации запросов, связанных с использованием ИС и обработки запросов заказчика по вопросам использования ИС и развертывания ИС у заказчика. Предоставление результатов анализа о влиянии запрошенных изменений на основные параметры проекта заинтересованным сторонам, и отчетности о записях конфигурационного управления: дефектах, запросах на изменение, проблемах

ПК-8.1: Демонстрирует знания современных подходов и стандартов автоматизации организации (например, CRM, MRP, ERP..., IITIL, ITSM). Методов и средств управления изменениями, качеством, персоналом, рисками, требованиями в проекте. Видов отчетности в проектах. Влияния организационного окружения на проект. Диаграммы Ганта, метода "набегающей волны", типов зависимостей между работами. Инструментов и методов выдачи и контроля поручений, моделирования бизнес-процессов в ИС. Устройства и функционирования современных ИС. Технологий выполнения работ по созданию (модификации) и сопровождению ИС. Основ теории систем и системного анализа.

ПК-8.2: Управляет работами в проекте. Анализирует исходную документацию. Контролирует исполнение выданных поручений. Подготавливает и представляет отчетность по проекту. Проводит рабочие и формальные согласования документации в проектах. Работает с системой контроля версий. Распределяет работы и выделяет ресурсы. Работает с рисками в проектах. Проводит переговоры и делает презентации
ПК-8.3: Владеет навыками внедрения инструментов и методов проведения приемо-сдаточных испытаний ИС. Выявления новых и отслеживания существующих рисков. Изменения и контроля плана выпуска релизов ИС на основе одобренных запросов на изменения. Контроля правильности расположения документации в репозитории проекта, именования и версионирования документов, фактического внесения изменений в элементы ИС. Назначения и распределения ресурсов. Обеспечения соответствия принятым в организации или проекте стандартам и технологиям. Определения необходимых изменений в ИС для реализации запроса. Организации: выполнения запросов на изменение и устранение несоответствий; передачи всех результатов проекта заказчику; согласования и утверждения требований с заинтересованными лицами. Оценки и предоставления результатов анализа влияния изменений в ИС на основные параметры проекта. Представления отчетности о записях конфигурационного управления: дефектах, запросах на изменение, проблемах. Разработки: планов проведения аудитов; правил именования и версионирования базовых элементов; правил использования репозитория проекта; предложений по улучшению шаблонов выходных документов об управлении проектами; регламентов закрытия запросов заказчика; типовых инструментов и методов распространения информации о ходе выполнения работ. Согласования: договоров и соглашений внутри организации; необходимости внесения изменений с заинтересованными сторонами и спонсором проекта; плана выпуска релизов ИС с заказчиком. Сравнения фактического исполнения проекта с планом управления и частными планами. Управления выпуском релизов ИС, сборкой программных базовых элементов конфигурации ИС. Фиксирования в системе учета факта внесения исправлений в архитектуру и дизайн ИС. Назначения членов команды проекта на выполнение работ в соответствии с планами и требуемой квалификацией. Организации формальной передачи результатов работ на следующую фазу ЖЦ проекта. Разработки отчета о проекте и обновление базы знаний организации. Разработки плана развития персонала в проекте, резервирования и архивирования репозитория проекта
ПК-6.1: Демонстрирует знания инструментов и методов интеграции ИС. Основ современных операционных систем. Возможностей и регламентов развертывания ИС. Инструментов и методов квалификационного аудита конфигурации ИС, модульного тестирования, тестирования нефункциональных и функциональных характеристик ИС, проектирования и дизайна ИС, согласования документации в проектах, физического и функционального аудита конфигурации ИС. **Программных средств и платформ инфраструктуры информационных технологий организаций. Систем контроля версий и поддержки конфигурационного управления. Современных методик тестирования разрабатываемых ИС. Технологий выполнения работ по созданию (модификации) и сопровождению ИС.**
ПК-6.2: Производит приемо-сдаточные испытания. Устанавливает права доступа на файлы и папки. Осуществляет интеграцию разработанного системного программного обеспечения.
ПК-6.3: Владеет навыками обеспечения соответствия процесса интеграции ИС у заказчика принятым в организации или проекте стандартам и технологиям. Внедрения инструментов и методов проведения приемо- сдаточных испытаний ИС. Выбора и разработки инструментов и методов проведения приемо-сдаточных испытаний ИС. Определения базовых элементов конфигурации ИС. Экспертной поддержки интеграции ИС с существующими ИС заказчика, оптимизации работы ИС. Присвоения версий базовым элементам конфигурации ИС. Управления сборкой программных базовых элементов конфигурации ИС
ПК-9.1: Демонстрирует знания архитектуры, устройства и функционирования вычислительных систем. Инструментов и методов верификации продукции или услуг в проектах в области ИТ. Инструментов и методов выявления требований, интеграции ИС, определения финансовых и производственных показателей деятельности организаций, оптимизации ИС, проведения приемо-сдаточных испытаний (валидации) ИС, согласования документации в проектах, управления требованиями. Методов формирования проектных команд. Основ менеджмента проектов, системного администрирования, теории управления, управления персоналом в организации. Программных средств и платформ инфраструктуры информационных технологий организаций. Регламента развертывания ИС. Систем контроля версий и поддержки конфигурационного управления. Современных инструментов и методов управления организацией, в том числе методов планирования деятельности, распределения поручений, контроля исполнения, принятия решений. Современных методик тестирования разрабатываемых ИС. Современных подходов и стандартов автоматизации организации (например, CRM, MRP, ERP..., IITIL, ITSM). Управления качеством: контрольные списки, верификация, валидация (приемо-сдаточные испытания. Устройства и функционирования современных ИС
ПК-9.2: Выполняет аудит конфигураций ИС. Контролирует исполнение регламентных документов. Планирует работы в проектах. Проверяет (верифицирует) архитектуру и дизайн ИС. Проводит переговоры, рабочие и формальные согласования документации в проектах. Производит приемо-сдаточные испытания. Работает с системой контроля версий. Распределяет работы и выделяет ресурсы. Управляет работами в проекте. Устанавливает права доступа на файлы и папки.

ПК-9.3: Владеет навыками выбора и разработки инструментов и методов разработки стратегии управления заинтересованными сторонами в проекте. Оценки эффективности мероприятий по развитию и управлению командой проекта. Получения необходимых ресурсов и управления ими для выполнения проекта (включая материальные, нематериальные, финансовые ресурсы, а также инструменты, оборудование и сооружения). Формулирования предложений по улучшению системы управления организацией в рамках инициированных корректирующих и предупреждающих действий. Разработки плана управления проектом и частных планов (управления качеством, персоналом, рисками, стоимостью, содержанием, временем, субподрядчиками, закупками, изменениями, коммуникациями). Разработки предложений по улучшению: управления финансами, персоналом, качеством; методики и шаблонов выходных документов управления проектами по созданию (модификации) и вводу в эксплуатацию ИС. Согласования плана управления: персоналом, документацией, изменениями, требованиями с заинтересованными сторонами проекта. Сравнения фактического исполнения проекта с планом управления проектом и частными планами (управления качеством, персоналом, рисками, стоимостью, содержанием, временем, субподрядчиками, закупками, изменениями, коммуникациями). Управления выпуском релизов ИС и сборкой программных базовых элементов конфигурации ИС. Утверждения плана управления: изменениями; рисками; требованиями; качеством

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Базовый перечень методов и средств защиты компьютерной информации.
3.1.2	Принципы классификации и примеры угроз безопасности компьютерным системам.
3.1.3	Современные отечественные и международные стандарты информационной безопасности информационных систем.
3.1.4	Наиболее распространённых алгоритмы и программные средства, и способов их применения при решении задач сокращения и противодействия рискам в области информационной безопасности.
3.1.5	Новые научные принципы и методы исследований рисков информационной безопасности.
3.1.6	Основные принципы разработки компонентов программно-аппаратных комплексов с учетом рисков информационной безопасности.
3.1.7	Архитектуру, устройство и функционирование вычислительных систем, современные методики тестирования разрабатываемых ИС. Современные стандарты информационного взаимодействия систем.
3.1.8	Современные подходы и стандарты противодействия рискам, возникающим при автоматизации организации.
3.1.9	Инструменты и методы интеграции информационных систем и возникающих при этом проблем информационной безопасности, а также проблемы сопровождения информационных систем.
3.1.10	Основ менеджмента проектов, системного администрирования, теории управления, управления персоналом в организации для исключения рисков в области информационной безопасности.
3.2	**Уметь:**
3.2.1	Реализовывать методы криптографической защиты информации в вычислительных системах;
3.2.2	Конфигурировать встроенные и дополнительные средства безопасности в операционной системе, локальных и глобальных сетях;
3.2.3	Устанавливать и настраивать программное обеспечение для защиты компьютерной информации.
3.2.4	Применять оригинальные алгоритмы и программы на основе использования математических методов для сокращения рисков информационной безопасности.
3.2.5	Применять на практике перспективные методики исследования прикладных и информационных процессов для предотвращения угроз информационной безопасности при проектировании и создании информационных систем.
3.2.6	Учитывать риски, возникающие при разработке компонентов программно-аппаратных комплексов обработки информации.
3.2.7	Выполнять аудит конфигураций информационных систем.
3.2.8	Работать с рисками в проектах.
3.2.9	Устанавливать права доступа на файлы и папки.
3.2.10	Выполнять аудит конфигураций информационной систем и выявлять риски.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Раздел 1					

1.1	Актуальность проблемы защиты информации. Основные факторы повышения рисков, связанных со способами сбора, обработки, представления информации и информационной культуры. Актуальность угроз и рисков связанных с составом и функциональными возможностями современных информационных технологий и программных средств /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-8.1 ПК-6.1 ПК-9.1 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.2	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации. Изучение различных информационно-коммуникационные технологии и их уровней безопасности. Факторы повышения угроз и рисков информационной безопасности систем на всех стадиях жизненного цикла информационных и автоматизированных систем. /Пр/	3	2	ПК-1.2 ПК-1.3 ПК-8.2 ПК-8.3 ПК-6.3 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.3	Актуальность проблемы защиты информации. Основные факторы повышения уАктуальность проблемы защиты информации. Основные факторы повышения рисков, связанных со способами сбора, обработки, представления информации и информационной культуры. Актуальность угроз и рисков связанных с составом и функциональными возможностями современных информационных технологий и программных средств.язвимости информации /Ср/	3	4	ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.4	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Базовый перечень законодательных актов. Отечественные и зарубежные стандарты информационной безопасности. Принципы использования законодательных норм. /Лек/	3	2	ПК-1.2 ПК-8.1 ПК-8.2 ПК-6.1 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.5	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Применение информационных технологий и программных средств, в том числе отечественного производства, и законодательное регулирование их применения. Отечественные и зарубежные стандарты информационной безопасности. /Пр/	3	2	ПК-1.2 ПК-1.3 ПК-8.2 ПК-8.3 ПК-6.2 ПК-6.3 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.6	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Базовый перечень законодательных актов. Отечественные и зарубежные стандарты информационной безопасности. Принципы использования законодательных норм. /Ср/	3	4	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.7	Проблемы защиты информации в информационных системах. Риски возникновения проблем защиты информации при проектировании и разработке информационных и автоматизированных систем. Различные способы сбора, обработки и представления информации с учетом современных требований информационной безопасности на всех уровнях жизненного цикла. /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-8.1 ПК-8.2 ПК-6.1 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.8	Проблемы защиты информации в информационных системах. Информационные технологии и программные средства защиты информации в информационных системах. Оценка рисков на различных этапах жизненного цикла. /Пр/	3	2	ПК-1.2 ПК-1.3 ПК-8.2 ПК-8.3 ПК-6.2 ПК-6.3 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.9	Проблемы защиты информации в информационных системах. Риски возникновения проблем защиты информации при проектировании и разработке информационных и автоматизированных систем. Различные способы сбора, обработки и представления информации с учетом современных требований информационной безопасности на всех уровнях жизненного цикла. /Ср/	3	4	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.10	Содержание системы средств защиты компьютерной информации в информационных системах. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-8.1 ПК-8.2 ПК-6.1 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.11	Содержание системы средств защиты компьютерной информации в АСОИУ. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Пр/	3	3	ПК-1.2 ПК-1.3 ПК-8.2 ПК-8.3 ПК-6.2 ПК-6.3 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.12	Содержание системы средств защиты компьютерной информации в информационных системах. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Ср/	3	3	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э5	
1.13	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Intenet.. /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-8.1 ПК-8.2 ПК-6.1 ПК-6.2 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.14	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Intenet /Пр/	3	2	ПК-1.2 ПК-1.3 ПК-8.2 ПК-8.3 ПК-6.2 ПК-6.3 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.15	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Intenet. /Ср/	3	3	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.16	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО /Лек/	3	2	ПК-1.1 ПК-1.2 ПК-8.1 ПК-8.2 ПК-6.1 ПК-6.2 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.17	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО. /Пр/	3	2	ПК-1.2 ПК-1.3 ПК-8.2 ПК-8.3 ПК-6.2 ПК-6.3 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.18	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО. /Ср/	3	3	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.19	Расчет и оценка рисков. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. /Лек/	3	3	ПК-1.1 ПК-1.2 ПК-8.1 ПК-8.2 ПК-6.1 ПК-6.2 ПК-9.1 ПК-9.2	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.20	Расчет и оценка рисков. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. /Пр/	3	2	ПК-1.2 ПК-1.3 ПК-8.2 ПК-8.3 ПК-6.2 ПК-6.3 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.21	Расчет и оценка рисков. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии. /Ср/	3	4	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.22	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. Защита информационных ресурсов от несанкционированного доступа. Внутримашинные средства /Лек/	3	1	ПК-1.1 ПК-1.2 ПК-8.1 ПК-8.2 ПК-6.1 ПК-6.2 ПК-9.1 ПК-9.2	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.23	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты информационных ресурсов от несанкционированного доступа. Внутримашинные средства. /Пр/	3	1	ПК-1.2 ПК-1.3 ПК-8.2 ПК-8.3 ПК-6.2 ПК-6.3 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.24	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. Защита информационных ресурсов от несанкционированного доступа. Внутримашинные средства. /Ср/	3	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.25	Контрольная работа /Контр.раб./	3	0		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Выполнение контрольной работы
1.26	Экзамен /Экзамен/	3	45	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-6.1 ПК-6.2 ПК-6.3 ПК-9.1 ПК-9.2 ПК-9.3	Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Вопросы к экзамен. Устный опрос.

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Оценочные материалы для текущего контроля и промежуточной аттестации

Представлены отдельным документом

5.2. Оценочные материалы для диагностического тестирования

Представлены отдельным документом

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Партыка Т. Л., Попов И. И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2018, электронный ресурс	1
Л1.2	Суворова Г. М.	Информационная безопасность: Учебное пособие для вузов	Москва: Юрайт, 2021, электронный ресурс	1

Л1.3	Сычев Ю.Н.	Защита информации и информационная безопасность: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2021, электронный ресурс	1
Л1.4	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2024, электронный ресурс	1

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Братановский С. Н., Лапин С. Ю.	Обеспечение доступа граждан к информации о деятельности органов государственной власти и местного самоуправления в Российской Федерации. Информационно-правовой аспект: Монография	Саратов: Электронно-библиотечная система IPRbooks, 2012, электронный ресурс	1
Л2.2	Гультяева Т. А.	Основы теории информации и криптографии: Конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2010, электронный ресурс	1
Л2.3	Бухтояров В. В., Золотарев В. В., Жуков В. Г.	Поддержка принятия решений при проектировании систем защиты информации: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014, электронный ресурс	1

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2015, электронный ресурс	1
Л3.2	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: Издательство "ФОРУМ", 2015, электронный ресурс	1

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	российский общеобразовательный портал
Э2	электронный журнал Открытые системы
Э3	сайт Информационных технологий
Э4	интернет-издание, посвященное новостям компьютерной индустрии, науки и техники.
Э5	журнал для ИТ-профессионалов.

6.3.1 Перечень программного обеспечения

6.3.1.1	MS Office
6.3.1.2	MS Visual Studio 2019

6.3.2 Перечень информационных справочных систем

6.3.2.1	Гарант-информационно-правовой портал. http://www.garant.ru/
6.3.2.2	
6.3.2.3	КонсультантПлюс –надежная правовая поддержка. http://www.consultant.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (лабораторных занятий), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации оснащена: комплект специализированной учебной мебели, маркерная (меловая) доска, комплект переносного мультимедийного оборудования - компьютер, проектор, проекционный экран, компьютеры с возможностью выхода в Интернет и доступом в электронную информационно-образовательную среду. Обеспечен доступ к сети Интернет и в электронную информационную среду организации.