Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков

« 10 » июля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Организационное и правовое обеспечение информационной безопасности
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: специалитет
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 288 (8)
(часы (ЗЕ))

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем
(код и наименование направления)

Направленность: Безопасность открытых информационных систем (СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель дисциплины - освоение дисциплинарных компетенций по применению ком-плекса мероприятий в системе защиты информации на основе реализации требований по правовой защите информации и организационному обеспечению информационной безопасности.
- изучение основных положений, понятий и категорий международных правовых документов Конституции и нормативно-правовых актов Российской Федерации в области обеспечения информационной безопасности;
- изучение правовых основ и принципов организации защиты государственной тайны и конфиденциальной информации, задач органов защиты государственной тайны и служб защиты информации на предприятиях;
- изучение организации работы и нормативных правовых актов и стандартов по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
- организация защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
- приобретение умений в разработке проектов нормативных и организационно-распорядительных документов в области обеспечения информационной безопасности и их применении;
- приобретение навыков работы в организации и обеспечении режима секретности, физической защиты объектов, методах организации работы с персоналом и управлению дея-тельностью служб защиты информации на предприятии.

1.2. Изучаемые объекты дисциплины

методы правовой защиты информации;
правовые основы защиты государственной, коммерческой, служебной, профессиональной тайны, персональных данных;
нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
правовая основа и порядок допуска и доступа к информации ограниченного доступа;
система правовой ответственности за правонарушения в информационной сфере;
правовые основы деятельности подразделений защиты информации;
порядок и принципы засекречивания и рассекречивания информации;
порядок организации охраны объектов информатизации, внутриобъектового и пропускного режима;
организация работы с персоналом по вопросам защиты информации;
организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам,
организация защиты информации в публикаторской и рекламной деятельности;
организация деятельности службы безопасности предприятия.

1.3. Входные требования

Не предусмотрены

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-5	ИД-1ОПК-5	Знает основы: нормативные документы в области российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных	Знает основы: нормативные документы в области технической защиты информации; основные документы по стандартизации в сфере управления ИБ; российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и ха¬рак¬те¬ри¬сти¬ку ос¬нов¬ных от-рас¬лей пра¬ва применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ОПК-5	ИД-2ОПК-5	Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации	Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации; формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы	Отчёт по практическому занятию
ОПК-5	ИД-3ОПК-5	Владеет навыками систематизации нормативных правовых	Владеет навыками систематизации нормативных правовых	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		актов, нормативных и методических документов, регламентирующих деятельность по защите информации	актов, нормативных и методических документов, регламентирующих деятельность по защите информации	
ОПК-6	ИД-1ОПК-6	Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя объекта информатизации в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	Отчёт по практическому занятию
ОПК-6	ИД-2ОПК-6	Умеет разрабатывать проекты инструкций, регламентов, положений	Умеет разрабатывать модели угроз и модели нарушителя объекта	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		и приказов, регламентирующих защиту информации ограниченного доступа в организации; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	информатизации в соответствии с нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации	
ОПК-6	ИД-3ОПК-6	Владеет навыками использования банка данных угроз безопасности ФСТЭК России	Владеет навыками использования специализированных баз данных ФСТЭК России	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		5	6
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	108	54	54
- лекции (Л)	48	24	24
- лабораторные работы (ЛР)			
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	56	28	28
- контроль самостоятельной работы (КСР)	4	2	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	108	54	54
2. Промежуточная аттестация			
Экзамен	72	36	36
Дифференцированный зачет			
Зачет			
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	288	144	144

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
5-й семестр				
Информационные отношения как объект правового регулирования	2	0	2	4
Структура информационной сферы и характеристика ее элементов. Информация как объект правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующие обеспечение информационной безопасности в Российской Федерации				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Правовой режим защиты государственной тайны	2	0	2	4
Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания				
Институт правовой защиты служебной тайны	2	0	2	4
Правовые основы защиты служебной тайны. Нормативно-правовые акты, регулирующие правовую защиту служебной тайны. Защита в режиме служебной тайны сведений, доступ к которым ограничивается в соответствии с законодательством, при обращении и хранении таких сведений (информации) в органах государственной власти и органах местного самоуправления. Защита служебной тайны в соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».				
Институт правовой защиты коммерческой тайны	2	0	2	6
Правовые основы защиты коммерческой тайны. Источники права о коммерческой тайне. Объекты и субъекты права на коммерческую тайну. Права и обязанности обладателя коммерческой тайны. Порядок установления режима коммерческой тайны при заключении и выполнении гражданско-правовых договоров. Юридическая защита права на коммерческую тайну. Ответственность за нарушение прав на коммерческую тайну.				
Институт правовой защиты профессиональной тайны	4	0	4	6
Понятие профессиональной тайны. Правовые основы защиты профессиональной тайны. Источники права о профессиональной тайне. Объекты и субъекты права на профессиональную тайну. Критерии охраноспособности права на профессиональную тайну. Права доверителя в отношении сведений, ставших на законных основаниях известными держателю профессиональной тайны. Особенности правовой защиты различных субинститутов профессиональной тайны. Правовые основы защиты банковской тайны. Источники права о банковской тайне. Объекты и субъекты права на				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
банковскую тайну. Права владельца банковской тайны в отношении сведений, составляющих его банковскую тайну. Обязанности пользователей банковской тайны				
Институт правовой защиты персональных данных	4	0	4	6
Правовые основы защиты информации персонального характера. Закон РФ «О персональных данных», подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных. Государственный надзор и контроль обработки персональных данных.				
Институт правовой защиты объектов критической информационной инфраструктуры	2	0	2	6
Правовые основы защиты объектов КИИ. Закон РФ «О безопасности критической информационной инфраструктуры», подзаконные нормативно-правовые документы о порядке защиты объектов КИИ. Государственный надзор и контроль защиты объектов КИИ.				
Государственное регулирование деятельности в области защиты информации	2	0	4	6
Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Правовые основы сертификации в области защиты информации.				
Правонарушения в информационной сфере и особенности защиты от них	2	0	2	6
Особенности правонарушений в информационной сфере. Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Правовая защита информационных систем.				
Правовая защита результатов интеллектуальной деятельности	2	0	4	6
Основы правовой защита результатов интеллектуальной деятельности. Институты права интеллектуальной собственности. Ответственность за нарушения норм права интеллектуальной собственности.				
ИТОГО по 5-му семестру	24	0	28	54

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
6-й семестр				
Понятие организационной защиты информации	2	0	2	4
Введение в организационное обеспечение информационной безопасности. Список рекомендованной литературы. Сущность организационных методов защиты информации. Соотношение организационных мер защиты информации с мерами правового и технического характера. Понятие «режим защиты информации».				
Организация режима секретности	2	0	2	4
Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Отличительные особенности системы организационной защиты государственной тайны. Распределение между уровнями государственного управления процессами защиты ГТ полномочий, управленческих функций и задач. Установление и изменение степени секретности сведений, отнесенных к государственной тайне. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Понятие «рассекречивание сведений». Основания для рассекречивания сведений, составляющих государственную тайну.				
Организация допуска и доступа к государственной тайне	2	0	2	4
Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование. Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности.				
Организация охраны объектов	2	0	4	6
Понятие «охрана». Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны. Виды, способы и особенности охраны различных объектов. Понятие о рубежах охраны. Многорубежная система охраны. Факторы выбора методов и средств охраны. Организация охраны объектов защиты в процессе их транспортировки				
Организация режимных мероприятий	2	0	2	6

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Понятие «режим», цели и задачи режимных мероприятий. Виды режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Виды пропускных документов. Порядок организации работы бюро пропусков. Контрольно-пропускные пункты, их оборудование и организация работы. Понятие «внутриобъектовый режим» и его общие требования. Противопожарный режим и его обеспечение.				
Организация работы с персоналом в системе защиты информации	4	0	4	6
Подбор и расстановка кадров. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Профессиональная ориентация и обучение персонала. Ознакомление сотрудника с правилами, процедурами и методами защиты информации. Организация обучения персонала. Основные формы обучения и методы контроля знаний. Мотивация персонала к выполнению требований по защите информации. Основные формы воздействия на персонал как методы мотивации: использование различных форм вознаграждения, управление карьерой, привлечение к участию в прибылях, воспитание «фирменного патриотизма» и др. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. Организационные меры по защите информации при увольнении сотрудника.				
Общий порядок организации работы с конфиденциальными документами	2	0	2	4
Основные понятия в области конфиденциального делопроизводства. Учет конфиденциальных документов, печатей, штампов и бланков. Специфика технологии защищенного документооборота.				
Порядок обработки входящих, исходящих и внутренних конфиденциальных документов	2	0	2	4
Порядок обработки входящих документов. Назначение и задачи стадии исполнения документов. Общие правила работы с конфиденциальными документами.				
Отдельные организационные аспекты обработки конфиденциальных документов	2	0	2	4

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Контроль исполнения конфиденциальных документов. Размножение конфиденциальных документов. Систематизация и оперативное хранение конфиденциальных документов и дел. Организация проверки наличия и уничтожения документов.				
Организационно-правовое обеспечение безопасной деятельности предприятий и организаций	2	0	2	6
Защита информации в сфере архивного делопроизводства. Правовые основы деятельности службы безопасности предприятия. Организационно-правовые основы использования электронной подписи.				
Организационные основы управления информационной безопасностью	2	0	4	6
Модели организационного управления ИБ. Организационная инфраструктура управления ИБ. Организационные мероприятия по управлению ИБ. Основы организации службы защиты информации.				
ИТОГО по 6-му семестру	24	0	28	54
ИТОГО по дисциплине	48	0	56	108

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Информационные отношения как объект правового регулирования
2	Правовой режим защиты государственной тайны
3	Институт правовой защиты служебной тайны
4	Институт правовой защиты коммерческой тайны
5	Институт правовой защиты профессиональной тайны
6	Институт правовой защиты банковской тайны
7	Институт правовой защиты персональных данных
8	Институт правовой защиты объектов критической информационной инфраструктуры
9	Формирование базы данных нормативно-правовых документов по защите информации (ПЗ)
10	Государственное регулирование деятельности в области защиты информации (ПЗ)
11	Преступления в сфере компьютерной информации (ПЗ)
12	Правовая защита результатов интеллектуальной деятельности (ПЗ)
13	Понятие и сущность организационной защиты информации

№ п.п.	Наименование темы практического (семинарского) занятия
14	Организация режима секретности
15	Организация допуска и доступа к сведениям, составляющим государственную тайну
16	Организация многорубежной системы охраны и физической защиты объекта информатизации (ПЗ)
17	Организация режимных мероприятий (ПЗ)
18	Организация работы с персоналом в системе защиты информации
19	Организация служебного расследования по фактам утраты информации (ПЗ)
20	Общие принципы организация работы с конфиденциальными документами
21	Порядок обработки входящих, исходящих и внутренних конфиденциальных документов (ПЗ)
22	Организация контроля исполнения конфиденциальных документов (ПЗ)
23	Организация использования СКСЗИ и средств электронной подписи
24	Организационные основы управления информационной безопасностью

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.

2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.

3. Особое внимание следует уделить выполнению отчетов по практическим занятиям и индивидуальным комплексным заданиям на самостоятельную работу.

4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Ажмухамедов И. М. Основы организационно-правового обеспечения информационной безопасности : учебное пособие / И. М. Ажмухамедов, О. М. Князева. - Санкт-Петербург: ИЦ Интермедия, 2017.	4
2	Данилов А. Н. Правовое обеспечение информационной безопасности : учебное пособие / А. Н. Данилов, А. С. Шабуров. - Пермь: Изд-во ПГТУ, 2008.	72
3	Организационно-правовое обеспечение информационной безопасности : учебное пособие для вузов / А. А. Стрельцов [и др.]. - Москва: Академия, 2008.	10
4	Основы организационного обеспечения информационной безопасности объектов информатизации : учебное пособие / С.Н. Семкин [и др.]. - Москва: Гелиос АРВ, 2005.	20
5	Романов О. А. Организационное обеспечение информационной безопасности : учебник для вузов / О. А. Романов, С. А. Бабин, С. Г. Жданов. - Москва: Академия, 2008.	7
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Анисимов А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. - Москва: ИНТУИТ, БИНОМ. Лаб. знаний, 2010.	2
2	Данилов А.Н. Организационное обеспечение информационной безопасности : учебное пособие / А.Н. Данилов, А.С. Шабуров. - Пермь: Изд-во ПГТУ, 2007.	83
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	ОРГАНИЗАЦИОННО-ПРАВОВОЕ И МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	https://moodle.kstu.ru/pluginfile.php/83871/mod_resource/content/1/1940.pdf	сеть Интернет; свободный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
База данных научной электронной библиотеки (eLIBRARY.RU)	https://elibrary.ru/
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
База данных компании EBSCO	https://www.ebsco.com/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	Мультимедийный проектор	1
Практическое занятие	Персональный компьютер	10

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Организационное и правовое обеспечение информационной безопасности»
Приложение к рабочей программе дисциплины

Направление подготовки: 10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы: Организация и технология защиты информации

Специальность: 10.05.03 Информационная безопасность автоматизированных систем
Специализация (профиль) образовательной программы: Безопасность открытых информационных систем

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 3 **Семестр**: 5,6

Трудоёмкость:
Кредитов по рабочему учебному плану: 8 ЗЕ
Часов по рабочему учебному плану: 288 ч.

Форма промежуточной аттестации:
Экзамен: 5,6 семестр

Пермь 2023

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение двух семестров (5-го, 6-го семестров учебного плана) и разбито на 6 учебных модулей. В каждом модуле предусмотрены аудиторные лекционные и практические занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по практическим заданиям и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы) для направления 10.03.01	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ПЗ**	**Т/КР**		**Экзамен**
Усвоенные знания						
3.1 Знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности		ТО1	ПЗ1 ПЗ2 ПЗ3 ПЗ4 ПЗ5 ПЗ6 ПЗ8 ПЗ9 ПЗ11	Т		ТВ
3.2 Знает систему нормативных правовых актов и		ТО2	ПЗ10			ТВ

стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа;			ПЗ14 ПЗ15			
З.3 Знает организационные меры по защите информации; основные методы управления защитой информации		ТО3				ТВ
Освоенные умения						
У.1 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации			ПЗ 2 ПЗ 3 ПЗ7 ПЗ12	Т		ПЗ
У.2 Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации			ПЗ 16 ПЗ 17			
У.3 Умеет осуществлять планирование и организацию работы персонала, с учетом требований по защите информации.			ПЗ 17 ПЗ 18 ПЗ 19			
Приобретенные владения						
В.1 Владеет навыками систематизации нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации			ПЗ 20 ПЗ 21 ПЗ 22	Т		КЗ
В.2 Владеет навыками использования специализированных баз данных ФСТЭК России			ПЗ9			КЗ
В.3 Владеет навыками выработки рекомендаций для принятия решения о модернизации систем защиты информации			ПЗ 23 ПЗ 24			КЗ

Контролируемые результаты обучения по дисциплине (ЗУВы) для специальности 10.05.03	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ПЗ**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знает основы: нормативные документы в области		ТО1	ПЗ1	Т		ТВ

технической защиты информации; основные документы по стандартизации в сфере управления ИБ; российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности			ПЗ2 ПЗ3 ПЗ4 ПЗ5 ПЗ6 ПЗ8 ПЗ9 ПЗ11			
З.2 Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа		ТО2	ПЗ10 ПЗ14 ПЗ15			ТВ
Освоенные умения						
У.1 Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации; формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации; формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации			ПЗ 2 ПЗ 3 ПЗ7 ПЗ12	Т		ПЗ
У.2 Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации			ПЗ 16 ПЗ 17 ПЗ 18 ПЗ 19			
У.3 Умеет осуществлять планирование и организацию работы персонала, с учетом требований по защите информации.						

Приобретенные владения						
В.1 Владеет навыками систематизации нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации			ПЗ 20 ПЗ 21 ПЗ 22	Т		КЗ
В.2 Владеет навыками использования специализированных баз данных ФСТЭК России			ПЗ9 ПЗ 23 ПЗ 24			КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;
- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;
- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;
- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса в рамках контроля самостоятельной работы студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания

заносятся в журнал преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

Вопросы для самостоятельного изучения:

Тема 1: Перспективы развития законодательства в области информационной безопасности.

Тема 2: Система контроля за состоянием защиты государственной тайны.

Тема 3: Порядок восстановления нарушенных информационных прав.

Тема 4: Практика совершенствования института сведений ограниченного распространения как основа для формирования и совершенствования института служебной тайны.

Тема 5: Права и обязанности органов государственной власти, иных государственных органов и органов местного самоуправления в отношении коммерческой тайны.

Тема 6: Защита владельцем банковской тайны своих прав.

Тема 7: Обязанности держателя профессиональной тайны. Защита доверителем своих прав.

Тема 8: Возможность использования закона «О частной детективной и охранной деятельности» для правовой защиты персональных данных.

Тема 9: Правовая регламентация сертификационной деятельности в области обеспечения информационной безопасности. Органы сертификации и их полномочия.

Тема 10: Практика расследования преступлений в сфере компьютерной информации.

Тема 11: Режим защиты информации как составная часть организационной защиты информации.

Тема 12: Категорирование объектов для организации защиты государственной тайны.

Тема 13: Особенности проведения инструктажа и документального оформления контракта о допуске к государственной тайне.

Тема 14: Безопасность при транспортировке носителей информации. Личная безопасность сотрудников и членов их семей.

Тема 15: Средства поиска и досмотра. Обнаружение металлов и взрывчатых веществ.

Тема 16: Документирование процедуры увольнения сотрудника.

Тема 17: Порядок реализации режимных мер в ходе проведения выездных конфиденциальных переговоров.

Тема 18: Обязанности лиц, участвующих в работе с иностранцами.

Тема 19: Порядок выявления каналов утечки информации при организации публикаторской деятельности.

Тема 20: Порядок создания и функционирования экспертных комиссий предприятий.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме

отчета по результатам практических заданий (после изучения каждого модуля учебной дисциплины).

Всего запланировано 24 практических занятия. Темы практических занятий приведены в РПД.

Отчет по выполнению практического задания проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний по разделу «Правовое обеспечение информационной безопасности»:

1. Структура информационной сферы, характеристика ее элементов.
2. Информация как объект правоотношений, категории информации.
3. Система правовой защиты информации.
4. Особенности государственной тайны как информации ограниченного доступа.
5. Засекречивание информации, отнесенной к государственной тайне.
6. Требования по защите сведений, отнесенных к государственной тайне.
7. Ответственность за нарушение режима секретности.
8. Понятие и основные виды конфиденциальной информации, в соответствии с требованиями российского законодательства.
9. Понятие и характеристика служебной тайны.
10. Нормативно - правовые основы защиты служебной тайны.
11. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения.
12. Правовые основы защиты коммерческой тайны.
13. Виды информации, составляющей коммерческую тайну.
14. Права и обязанности обладателя коммерческой тайны.
15. Основные угрозы коммерческой тайны.
16. Особенности правовой защиты коммерческой тайны.
17. Понятие и правовые основы профессиональной тайны.
18. Нотариальная тайна и особенности ее правовой защиты. Тайна завещания.

19. Врачебная тайна и особенности ее правовой защиты.
20. Адвокатская тайна и особенности ее правовой защиты.
21. Аудиторская тайна и особенности ее правовой защиты.
22. Тайна страхования и особенности ее правовой защиты. Тайна ломбарда.
23. Тайна связи и особенности ее правовой защиты. Тайна переписки, почтовых, телеграфных и иных сообщений.
24. Правовые основы защиты банковской тайны. Раскрытие информации, относящейся к банковской тайне.
25. Нарушение банковской тайны и ответственность за подобные нарушения.
26. Формирование российского законодательства в области защиты персональных данных.
27. Основные понятия и содержание закона РФ «О персональных данных».
28. Подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.
29. Государственный надзор и контроль обработки персональных данных, ответственность за нарушения российского законодательства в данной области.
30. Основные понятия, термины и определения в области обеспечения безопасности объектов КИИ. Права и обязанности субъектов КИИ.
31. Состав законов РФ и указов Президента РФ в области безопасности КИИ.
32. Состав постановлений Правительства РФ в области безопасности КИИ.
33. Приказы ФСТЭК России и ФСБ России в области безопасности КИИ.
34. Государственный надзор и контроль защиты объектов КИИ.
35. Ответственность за нарушение законодательства о безопасности КИИ РФ.
36. Правовые основы лицензирования в области защиты информации.
37. Правовые основы сертификации в области защиты информации.
38. Особенности правонарушений в информационной сфере.
39. Преступления в сфере компьютерной информации: виды, состав.
40. Основы расследования преступлений в сфере компьютерной информации.
41. Требования отечественных стандартов по защите информационных систем.
42. Приказы и специальные нормативные документы ФСТЭК России по защите информационных систем.
43. Правовые основы применения электронной подписи.
44. Правовая защита результатов интеллектуальной деятельности.
45. Результаты интеллектуальной деятельности.
46. Авторское и смежное право.
47. Технические средства защиты авторских прав.
48. Патентное право.
49. Право на селекционное достижение, на топологии интегральных микросхем, на секрет производства (ноу-хау).
50. Права на средства индивидуализации.

Типовые вопросы для контроля усвоенных знаний по разделу «Организационное обеспечение информационной безопасности»:

1. Понятие и основные направления организационной защиты информации. Соотношение организационных мер по защите информации с мерами правового и технического характера.

2. Организация защиты информации, в соответствии с ISO/IEC 27002. Внутренние и внешние стороны организации.
3. Основные термины, связанные с организацией защиты информации.
4. Понятие системы защиты государственной тайны в Российской Федерации и ее составляющие.
5. Развитие системы организационной защиты государственной тайны в Российской Федерации.
6. Органы защиты государственной тайны в Российской Федерации и их основные функции.
7. Объекты, средства и цели защиты сведений, составляющих государственную тайну.
8. Основные меры по информационной безопасности при организации защиты сведений, составляющих государственную тайну.
9. Высшие учебные заведения как элемент системы защиты государственной тайны в Российской Федерации.
10. Режим секретности. Основные функции в деятельности режимно-секретных подразделений организации.
11. Отнесение сведений к государственной тайне (засекречивание). Критерии для отнесения сведений к государственной тайне.
12. Рассекречивание сведений и их носителей. Основания и порядок рассекречивания сведений, составляющих государственную тайну.
13. Порядок допуска к сведениям, составляющим государственную тайну.
14. Основания для отказа гражданину в допуске к государственной тайне.
15. Особенности проведения проверочных мероприятий для допуска к сведениям, составляющим государственную тайну.
16. Основания для прекращения допуска к сведениям, составляющим государственную тайну.
17. Порядок оформления допуска к государственной тайне. Основные учетные формы.
18. Организация доступа к сведениям, составляющим государственную тайну.
19. Понятие организации охраны, цели и задачи охранной деятельности.
20. Объекты охраны. Понятие системы охраны предприятия и состав ее компонентов.
21. Понятие физической защиты информации и организация системы охраны.
22. Организация физической безопасности, в соответствии с ISO/IEC 27002.
23. Понятие многорубежной системы охраны. Рубежи и зоны безопасности.
24. Понятие «режим», его цели задачи и разновидности.
25. Организация пропускного режима. Состав пропускных документов.
26. Порядок организации работы бюро пропусков и контрольно-пропускных пунктов.
27. Организация внутриобъектового и противопожарного режима. Требования, предъявляемые к режимным помещениям.
28. Содержание этапов подбора персонала на должности, предполагающие допуск к конфиденциальной информации.

29. Особенности организации трудоустройства должностных лиц, допускаемых к конфиденциальной информации.
30. Перечень и содержание документов, определяющих порядок работы с конфиденциальной информацией.
31. Организация обучения персонала. Основные формы обучения и методы контроля знаний. Организация и проведение киберучений.
32. Воспитание персонала как гарантия выполнения требований по защите информации. Основные формы воздействия на персонал и методы мотивации.
33. Организация контроля персонала. Основные формы и методы контроля. Анализ степени осведомленности работников.
34. Порядок организации и проведения служебного расследования по факту утраты конфиденциальной информации.
35. Основные меры по защите информации при увольнении сотрудника.
36. Учет конфиденциальных документов, печатей, штампов и бланков.
37. Контроль исполнения конфиденциальных документов.
38. Размножение конфиденциальных документов.
39. Систематизация и оперативное хранение конфиденциальных документов и дел.
40. Организация проверки наличия и уничтожения документов.
41. Определение уровней защищенности ПДн. Формирование и выполнение требований по защите персональных данных в ИС ПДн.
42. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных.
43. Система нормативных правовых актов по вопросам обеспечения безопасности КИИ РФ.
44. Система «ГосСОПКА»: понятие, структура, основные функции.
45. Основные мероприятия по категорированию объектов КИИ.
46. Порядок формирования требований по обеспечению защиты значимых объектов КИИ.
47. Требования к созданию систем безопасности значимых объектов КИИ.
48. Модели организационного управления информационной безопасностью.
49. Организационная инфраструктура и организационные мероприятия по управлению информационной безопасностью.
50. Основы организации службы защиты информации.

Типовые практические задания для контроля освоенных умений:

1. В роли администратора информационной безопасности разработать Перечень сведений конфиденциального характера для коммерческого предприятия.
2. Определить виды и степени ответственности за правонарушения и преступления в информационной сфере на основе действующего законодательства.
3. Организовать работы по проверке кандидатов на должность, текущей работы с персоналом по обеспечению информационной безопасности
4. Подготовить проведение мероприятий, проводимых при увольнении сотрудника.
5. Подготовить данные для регистрации оператора ПДн в Едином реестре операторов ПДн на примере обработки одной ИС ПДн.

6. Для одной ИСПДн определить уровень защищенности (УЗ) ПДн, с оформлением соответствующего акта.
7. Определить и обосновать состав базовых мер по защите информации для ИСПДн, в соответствии с Постановлением Правительства РФ №1119, Приказом ФСТЭК №21 на основании определенного УЗ ИСПДн.
8. Разработать проект Положения по обработке персональных данных для предприятия (организации).
9. В роли администратора информационной безопасности разработать предложения и задачи должностным лицам по подготовке к инспекции Роскомнадзора на предмет контроля обработки персональных данных.
10. Разработать план мероприятий по проведению категорирования объекта КИИ.
11. Определить состав комиссии предприятия по проведению категорирования объекта КИИ.
12. Разработать Перечень объектов КИИ, подлежащих категорированию субъекта КИИ.
13. Оценить показатели критериев значимости объекта КИИ.
14. Составить Акт категорирования объекта КИИ.
15. Составить перечень действий по определению состава системы безопасности значимого объекта КИИ.

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в

оценочный лист и заполняются преподавателем по итогам промежуточной аттестации. Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы. При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.

Контрольно - измерительные материалы (тестовые задания) по дисциплине «Организационно-правовое обеспечение информационной безопасности»

1. Понятие национальной безопасности Российской Федерации определено:

   Доктриной национальной безопасности Российской Федерации;
   Стратегией национальной безопасности Российской Федерации;
   Доктриной информационной безопасности Российской Федерации;
   Конституцией Российской Федерации.

2. Состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах личности, общества и государства, называется:

   –
   национальной безопасностью Российской Федерации;
   информационной безопасностью Российской Федерации;
   информационной защитой Российской Федерации;
   защитой информации в информационной сфере.

3. К составляющим национальных интересов РФ в информационной сфере, определенных Доктриной информационной безопасности не относится:

   –
   соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;
   противодействие иностранным техническим разведкам;
   развитие современных информационных технологий;
   защита информационных ресурсов от несанкционированного доступа.

4. Совокупностью решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание и функционирование систем защиты информации на конкретных объектах, называется:

   –
   нормативное обеспечение информационной безопасности;
   правовое обеспечение информационной безопасности;
   организационное обеспечение информационной безопасности;
   организационно-правое обеспечение информационной безопасности.

5. Основным принципом отнесения информации к информации ограниченного распространения не является:

   –
   ограничивать доступ к информации может только ее собственник или уполномоченные им на то лица;
   обязательное использование автоматизированных средств обработки;
   чем важнее для собственника информация, тем тщательнее он ее защищает;
   защищают и охраняют наиболее важную, ценную для собственника информацию.

6. К подзаконным нормативно-правовым актам не относятся:

   –
   указы Президента;
   международные договоры;
   постановления Правительства;
   ведомственные инструкции.

7. Совокупность правовых норм, регулирующих определенную область общественных отношений, называется:

   –
   отраслью права;
   подотраслью права;
   институтом права;
   нормой права.

8. К регулятивным отраслям права не относится:

   –
   Конституционное право;
   Уголовное право;

Административное право;
Экологическое право.

_

9. К охранительным отраслям права не относится:

_

Уголовно-процессуальное право;
Трудовое право;
Уголовное право;
Арбитражно-процессуальное право.

_

10. Система норм, регулирующих отношения между государствами в процессе их борьбы и сотрудничества, а также система норм, регулирующих гражданско-правовые, семейные и трудовые отношения с иностранным или международным элементом, называется:

_

межгосударственным правом;
международным правом;
интернациональным правом;
правом межгосударственных отношений.

_

11. Основным старейшим международным документом по патентованию и защите интеллектуальной собственности, является**:**

_

Соглашение по торговым аспектам прав интеллектуальной собственности;
Парижская конвенция по охране промышленной собственности;
Договор о патентной кооперации;
Страсбургское соглашение по вопросам международной патентной кооперации.

_

12. Информационная безопасность подразумевает обеспечение:

_

целостности, доступности, своевременности информации;
целостности, доступности, конфиденциальности информации;
достоверности, конфиденциальности, доступности информации;
конфиденциальности, достоверности, избыточности информации.

_

13. Двуединство информации и материального носителя дает возможность защищать документированную информацию с использованием одновременно двух институтов:

_

институтов гражданской и материальной собственности;
институтов интеллектуальной и вещной собственности;
институтов интеллектуальной и частной собственности;
институтов гражданской и вещной собственности.

_

14. Информация в зависимости от категории доступа к ней подразделяется на:

_

три категории;
две категории;
четыре категории;
пять категорий.

_

15. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

_

три категории;
четыре категории;
пять категорий;
две категории.

_

16. К основным конституционным гарантиям информационных прав не относится:

_

законы подлежат официальному опубликованию;
право на ознакомление с информацией ограниченного распространения;
право каждого на самозащиту своих прав;
право на достоверную информацию о состоянии окружающей среды.

_

17. К принятым в Российской Федерации законодательным актам в области информационной безопасности не относится закон:

    –
    «О государственной тайне»;
    «О профессиональной тайне»;
    «О коммерческой тайне»;
    «О безопасности».

    –
18. Свойством конфиденциальности не обладает:

    –
    коммерческая тайна;
    государственная тайна;
    банковская тайна;
    служебная тайна.

    –
19. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен:

    –
    специальным перечнем;
    федеральными законами;
    собственником информации;
    техническими средствами защиты информации.

    –
20. Перечень сведений, отнесенных к государственной тайне, определяется:

    –
    постановлением Правительства Российской Федерации;
    указом Президента Российской Федерации;
    законом Российской Федерации «О государственной тайне»;
    Доктриной информационной безопасности Российской Федерации.

    –
21. Сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях, следует относить к:

    –
    секретным;
    совершенно секретным;
    особой важности;
    конфиденциальным.

    –
22. В структуру государственной системы защиты информации не входят:

    –
    структурные и межотраслевые подразделения по защите информации органов государственной власти;
    ФАПСИ при Президенте РФ, и его подразделения по защите информации;
    предприятия, специализирующиеся на проведении работ в области защиты информации;
    МВД и его подразделения по защите информации.

    –
23. Отнесение сведений к государственной тайне и их засекречивания базируется на соответствующей системе принципов:

    –
    законности, обоснованности и достоверности;
    законности, обоснованности и своевременности;
    обоснованности, своевременности и конфиденциальности;
    законности, достоверности и доступности.

    –
24. Не подлежат засекречиванию сведения:

    –
    о чрезвычайных происшествиях на объектах вооружения и военной техники;
    о размерах золотого запаса и государственных валютных резервах Российской Федерации;
    о состоянии здоровья первых должностных лиц органов государственной власти;
    о расходах бюджета Российской Федерации.

    –
25. На носители сведений, составляющих ГТ, не наносится реквизит:

    –
    об органе государственной власти, о предприятии, об учреждении, организации, осуществивших засекречивание носителя;
    о дате засекречивания сведений;

о регистрационном номере;
о дате или условии рассекречивания сведений.

–

26. Информация, содержащая сведения, отнесенные к государственной или служебной тайне, должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты:

–
защищенных от несанкционированного доступа;
сертифицированных в установленном порядке;
аттестованных установленным порядком;
исключающих побочные электромагнитные излучения.

–

27. Служебная тайна в первую очередь связана с интересами:

–
воинской службы;
государственной службы и службы в органах местного самоуправления;
государственной гражданской службы;
государственной службы в органах государственной власти.

–

28. Не могут быть отнесены к служебной тайне:

–
сведения содержащие персональные данные граждан Российской Федерации;
описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;
документы, накапливаемые в фондах библиотек и архивов;
сведения об отдельных статьях расходов бюджета Российской Федерации.

–

29. Нормативно - правовые основы защиты служебной тайны не определены:

–
Гражданским кодексом Российской Федерации;
Административным кодексом Российской Федерации;
Налоговым кодексом Российской Федерации;
Таможенным кодексом Российской Федерации.

–

30. На документах или на их проектах, содержащих служебную информацию ограниченного распространения, проставляется пометка:

–
«Налоговая тайна»;
«Для служебного пользования»;
«Конфиденциально»;
«Секретно».

–