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

« 29 » мая 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Организационно-правовые механизмы обеспечения информационной безопасности
(наименование)

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

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

Общая трудоёмкость: 180 (5)
(часы (ЗЕ))

Направление подготовки: 10.04.01 Информационная безопасность
(код и наименование направления)

Направленность: Комплексные системы информационной безопасности
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель дисциплины - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе реализации требований по организационно-правовому обеспечению информационной безопасности
Задачи дисциплины:
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 тай-ны и конфиденциальной информации с целью;
изучение организации работы и порядка применения нормативных правовых актов и стандартов по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, аттестации объектов информатизации и сертификации средств защиты информации;
формирование умений в разработке проектов нормативных и организационно-распорядительных документов в области защиты информации и их применении на основе анализа угроз информационной безопасности объектов и разработке методов противодействия угрозам информационной безопасности;
формирование навыков работы в организации физической защиты объектов, методах организации работы с персоналом и управлению деятельностью по защите информации, при необходимости проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности.

1.2. Изучаемые объекты дисциплины

методы правовой защиты информации;
правовые основы защиты государственной, коммерческой, служебной, профессиональной тайны, персональных данных;
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

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-2.1	ИД-1ПК-2.1	Знает правовые и организационные основы разработки и внедрения систем защиты информации программного обеспечения автоматизированных систем.	Знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем.	Отчёт по практическому занятию
ПК-2.1	ИД-2ПК-2.1	Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах.	Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах.	Отчёт по практическому занятию
ПК-2.1	ИД-3ПК-2.1	Владеет навыками составления организационно-правовых механизмов по оценке рисков информационной безопасности в автоматизированных системах и формированию перечня информационных ресурсов и объектов, подлежащие защите	Владеет навыками оценивания информационных рисков в автоматизированных системах и опреде-ления информационной инфраструктуры и информационных ресурсов, подлежащие защите	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		2
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	18	18
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	34	34
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	90	90
2. Промежуточная аттестация		
Экзамен	36	36
Дифференцированный зачет		
Зачет		
Курсовой проект (КП)		
Курсовая работа (КР)		
Общая трудоемкость дисциплины	180	180

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
2-й семестр				
Информационные отношения как объект правового регулирования	2	0	2	10
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				

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	4	10
Понятие правового режима защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государ-ственную 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. Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Особенности системы организационной защиты государственной тайны. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны. Организация деятельности режимно-секретных органов. Установление и изменение степени секретности сведений, отнесенных к государственной тайне. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.				
Правовой режим защиты информации конфиденциального характера	2	0	4	10
Понятие информации конфиденциального характера по российскому законодательству. Основные виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судо-производства. Правовой режим конфиденциальной информации: содержание и особенно-сти. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Нормативные и организационно-распорядительные документы, регламентирующие работу по защите информации				
Институт правовой защиты персональных данных	2	0	4	10
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.				
Государственное регулирование деятельности в области защиты информации	2	0	4	10
Понятие лицензирования по российскому				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обес-печения информационной безопасности. Объекты лицензирования и участники лицензион-ных 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. 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				
Организация охраны и режма	2	0	4	10
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. Понятие «режим», цели и задачи режимных мероприятий. Виды режима. Организация про-пускного 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.				
работа с персоналом, обладающим конфиденциальной информацией	2	0	4	10
Подбор и расстановка кадров. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Организация обучения персонала. Основные формы обу-чения и методы контроля знаний. Мотивация персонала к выполнению требований по за-щите информации. Основные формы воздействия на персонал как методы мотивации: воз-награждение, управление карьерой, профессиональная этика. Организация контроля соблю-дения персоналом требований				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
режима защиты информации. Методы проверки персонала. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. Организационные меры по защите информации при увольнении со-рудника.				
Организация подготовки и проведения конфиденциальных переговоров	2	0	4	10
Основные требования, предъявляемые к подготовке и проведению конфиденциальных пе-реговоров. Основные этапы проведения конфиденциальных переговоров. Подготовка по-мещения для проведения конфиденциальных переговоров. Подготовка программы проведения конфиденциальных переговоров. Порядок встречи и регистрации приглашенных лиц. Порядок проведения конфиденциальных переговоров. Организация конфиденциального делопроизводства				
Организация работы службы безопасности предприятия	2	0	4	10
Концепция безопасности предприятия (организации) и ее содержание. Политика информа-ционной безопасности. Подразделения, обеспечивающие ИБ предприятия: основные функ-ции, содержание деятельности, структура, обязанности сотрудников. Варианты организационных структур, обеспечивающих защиту информации. Основные документы службы ин-формационной безопасности.				
ИТОГО по 2-му семестру	18	0	34	90
ИТОГО по дисциплине	18	0	34	90

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Информационные отношения как объект правового регулирования.
2	Правовой режим защиты государственной и служебной тайны. Организация режима секретности
3	Нормативные и организационно-распорядительные документы, регламентирующие работу по защите информации (ПЗ)
4	Организационно-правовые механизмы защиты коммерческой тайны
5	Институт правовой защиты персональных данных
6	Организационно-правовые механизмы защиты персональных данных

№ п.п.	Наименование темы практического (семинарского) занятия
7	Государственное регулирование деятельности в области защиты информации (ПЗ)
8	Организация процедур лицензирования и сертификции по защите информации
9	Пресечение нарушений в сфере компьютерной информации (ПЗ)
10	Правовая защита информационных систем (ПЗ)
11	Организация многорубежной системы охраны и физической защиты информации(ПЗ)
12	Порядок организации режимных мероприятий (ПЗ)
13	Порядок организации работы с персоналом в системе защиты информации (ПЗ)
14	Организация служебного расследования по фактам утраты информа-ции (ПЗ)
15	Порядок организации конфиденциального делопроизводства и документооборота
16	Организация защиты информации при организации конфиденциальных переговоров, приеме посетителей и командированных лиц (ПЗ)
17	Организация работы службы безопасности предприятия (ПЗ)

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при которой 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 установления 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, лабораторным работам 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	Данилов А. Н. Правовое обеспечение информационной безопасности : учебное пособие / А. Н. Данилов, А. С. Шабуров. - Пермь: Изд-во ПГТУ, 2008.	73
2	Данилов А.Н. Организационное обеспечение информационной безопасности : учебное пособие / А.Н. Данилов, А.С. Шабуров. - Пермь: Изд-во ПГТУ, 2007.	83
3	Северин В.А. Правовая защита информации в коммерческих организациях : учебное пособие для вузов / В.А. Северин. - Москва: Академия, 2009.	4
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Организационно-правовое обеспечение информационной безопасности : учебное пособие для вузов / А. А. Стрельцов [и др.]. - Москва: Академия, 2008.	10
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	Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-систем	http://vestnik.pstu.ru/get/_res/fs/file.pdf/5874/%D8%E0%E1%F3%F0%EE%E2+%C0.%D1.%2C+%C1%EE%F0%E8%F1%EE%E2+%C2.%C8.+%D0%E0%E7%F0%E0%E1%EE%F2%EA%E0+%EC%EE%E4%E5%EB%E8+%E7%E0%F9%E8%F2%FB+%E8%ED%F4%EE%F0%EC%E0%F6%E8%E8+%EA%EE%F0%EF%EE%F0%E0%F2%E8%E2%ED%EE%E9+%	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
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
Лекция	Мультимедийный роектор	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 «Организационно-правовые механизмы обеспечения информационной безопасности»
Приложение к рабочей программе дисциплины

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) образовательной программы: Комплексные системы информационной безопасности

Квалификация выпускника: Магистр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 1 **Семестр**: 2

Трудоёмкость:
Кредитов по рабочему учебному плану: 5 ЗЕ
Часов по рабочему учебному плану: 180 ч.

Форма промежуточной аттестации:
Экзамен: 2 семестр

Пермь 2021

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 одного семестра (2-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и лабораторные 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 лабораторным работам и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ОЛР**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем				Т1 Т2 Т3		ТВ
Освоенные умения						
У.1 Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах.						ПЗ
В.1 Владеет навыками оценивания информационных рисков в автоматизированных системах, определения информационной инфраструктуры и информационных ресурсов, подлежащие защите						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 студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты практических работ (после изучения каждого модуля учебной дисциплины).

Всего запланировано 17 практических занятий. Темы практических занятий приведены в РПД.

Защита результатов работы 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 отчетов по практическим занятиям 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:

1. Структура информационной сферы и характеристикаее элементов.
2. Информация как объект правоотношений. Цифровые права.
3. Категории информации по условиям доступа к ней и распространения.
4. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
5. Субъекты и объекты правоотношений в области информационной безопасности.
6. Понятие правового режима защиты государственной тайны.
7. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.
8. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
9. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
10. Организационные меры, направленные на защиту государственной тайны.
11. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
12. Особенности системы организационной защиты государственной тайны. Распределение между уровнями государственного управления полномочий, управленческих функций изадач по защите государственной тайны.
13. Организация деятельности режимно-секретных органов.
14. Установление и изменение степени секретности сведений, отнесенных к государственной тайне. Понятие «рассекречивание сведений». Основания для рассекречивания сведений.
15. Понятие информации конфиденциального характера по российскому законодательству. Основные виды конфиденциальной информации:

персональные данные, служебная тайна, коммерческая тайна, банковская тайна, профессиональная тайна, тайна следствия и судопроизводства.

16. Правовой режим конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
17. Нормативные и организационно- распорядительные документы, регламентирующие работу по защите информации.
18. Правовые основы защиты информации персонального характера. Закон РФ «О персональных данных», подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.
19. Государственный надзор и контроль обработки персональных данных.
20. Понятие лицензирования. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности.
21. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия.
22. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности.
23. Правовые основы сертификации в области защиты информации.
24. Особенности правонарушений в информационной сфере.
25. Преступления в сфере компьютерной информации: виды, состав.
26. Основы расследования преступлений в сфере компьютерной информации.
27. Правовая защита информационных систем.
28. Правовая защита результатов интеллектуальной деятельности.
29. Понятие «охрана». Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, материальные и финансовые ценности. Особенности их охраны.
30. Виды, способы и особенности охраны различных объектов. Понятие о рубежах охраны.
31. Многорубежная система охраны. Факторы выбора методов и средств охраны.
32. Понятие «режим», цели и задачи режимных мероприятий. Виды режима.
33. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков.
34. Виды пропускных документов. Порядок организации работы бюро пропусков
35. Контрольно- пропускные пункты, их оборудование и организация работы.
36. Понятие «внутриобъектовый режим» и его общие требования. Противопожарный режим и его обеспечение.
37. Основные мероприятия по защите информации при подборе и расстановке кадров.
38. Направления и методы работы с персоналом, обладающим конфиденциальной информацией.
39. Организация обучения персонала. Основные формы обучения и методы контроля знаний.
40. Мотивация персонала к выполнению требований по защите информации.

Основные формы воздействия на персонал как методы мотивации: вознаграждение, управление карьерой, профессиональная этика.

41. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.
42. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.
43. Организационные меры по защите информации при увольнении сотрудника.
44. Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров. Основные этапы проведения конфиденциальных переговоров.
45. Подготовка помещения для проведения конфиденциальных переговоров и программы проведения конфиденциальных переговоров.
46. Порядок встречи и регистрации приглашенных лиц. Порядок проведения конфиденциальных переговоров.
47. Организация конфиденциального делопроизводства.
48. Концепция безопасности предприятия (организации) и ее содержание. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
49. Модели организационного управления информационной безопасностью.
50. Варианты организационных структур, обеспечивающих защиту информации. Основные документы службы информационной безопасности.

Типовые вопросы и практические задания для контроля освоенных умений:

1. В роли администратора информационной безопасности подготовить предложения по подготовке предприятия (организации) к инспекции Роскомнадзора, для чего:

– Перечислить основные этапы деятельности на предприятии (в организации) по организации защиты персональных данных.
– Определить и обосновать состав ИСПДн предприятия (организации).
– Подготовить данные для регистрации оператора ПДн в Едином реестре операторов ПДн.
– Определить и обосновать решения по защите информации (технической, криптографической, физической) для ИСПДн предприятия (организации).
– Перечислить состав нормативно-методического обеспечения защиты персональных данных на предприятии (в организации). Разработать проект Положения по обработке персональных данных для предприятия (организации).

2. Подготовить перечень документов, направляемых соискателем лицензии на техническую защиту конфиденциальной информации.
3. **Разработать:**
   – алгоритм проведения сертификации средства защиты информации, с учетом всех необходимых процедур по сертификации;
   – перечень документов по сертификации средств защиты информации, включая профили защиты для средств защиты информации.

4. **В роли администратора информационной безопасности подготовить предложения по:**
   - расследованию инцидента, связанного с модификацией компьютерной информации ограниченного доступа;

оценке последствий нарушений:

   - законодательства Российской Федерации в области персональных данных;
   - правил защиты информации;
   - незаконной деятельности в области защиты информации;
   - разглашения информации с ограниченным доступом.

5. Разработать:
   - Предложения по организации системы охраны объекта на каждом рубеже (с учетом возможного применения сил средств и методов охраны, выполнения требований ГОСТ Р ИСО/МЭК 27002).
   - Подготовить решение по организации охраны объекта информатизации, с учетом привлечения специализированных предприятий.

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.