МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

По направлению подготовки 10.03.01 «Информационная безопасность»
профиль «Безопасность автоматизированных систем»

Уровень квалификации выпускника (*бакалавр*)
Форма обучения (*очная*)

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2021

Организационное и правовое обеспечение
информационной безопасности.
Организационное обеспечение информационной безопасности
Рабочая программа дисциплины
Составитель:
к.и.н., доцент, кафедры
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 10 от 20.05.2021

ОГЛАВЛЕНИЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Пояснительная записка

1.1. Цель и задачи дисциплины (модуля)

Содержание дисциплины охватывает круг вопросов, связанных с теоретическими и практическими проблемами формирования и функционирования систем организационного и правового обеспечения информационной безопасности, а также формированием практических навыков по организационной защите информации и применению норм права в области информационной безопасности.

Цель курса: формирование знаний по теоретическим и практическим проблемам функционирования систем организационного и правового обеспечения информационной безопасности с целью формирования практических навыков по организационной защите информации и применению норм права в области информационной безопасности. Способствовать в подготовке специалиста, умеющего сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельность, основу которой составляет организационная работа.

Задачи курса:

- изучить базовые теоретические понятия, лежащие в основе мероприятий по организационному и правовому обеспечению информационной безопасности;

- овладеть практическими организационными методами защиты информации на объектах информатизации;

- овладеть необходимой юридической терминологией;

- сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельность, основу которой составляет организационная работа.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине *(модулю)*:

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм,	УК-2.1 Уметь анализировать имеющиеся ресурсы и ограничения, оценивать и выбирать оптимальные способы решения поставленных задач	Знать сущность информации, методы и способы её отражения и передачи; Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать основы правовых
	УК-2.2 Уметь использовать знаний о важнейших нормах,	

имеющихся ресурсов и ограничений	институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.	знаний в различных сферах деятельности
ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;	ОПК-5.1 Уметь применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	
	ОПК-5.2 Уметь обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав	
	ОПК-5.3 Владеть навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации	
ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и	ОПК-6.1 Знать нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать: основы информационного права, сущность конфиденциальности информации и знать виды носителей информации и особенности фиксации на них информации; сущность информации, методы и способы её отражения и передачи; закономерности развития предприятий различного типа и организацию их функционирования с целью
	ОПК-6.2 Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации	

методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ограниченного доступа в организации	достижения максимальной эффективности при минимальных затратах ресурсов. Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать основы правовых знаний в различных сферах деятельности
	ОПК-6.3 Владеет навыками по разработке политики безопасности объекта информатизации	

1.3.Место дисциплины в структуре основной образовательной программы

Дисциплина (модуль) «Организационное обеспечение информационной безопасности» входит в базовую часть цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность». Дисциплина реализуется кафедрой Информационной безопасности.

Для освоения дисциплины (модуля) необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Правовое обеспечение информационной безопасности», «Основы информационной безопасности».

В результате освоения дисциплины (модуля) формируются знания, умения и владения, необходимые для прохождения дисциплин «Защита информации от несанкционированного доступа» и «Системы контроля и управления доступом», «Аудит информационной безопасности», «Системы управления информационной безопасности».

2. Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 4 з. е., 152 ч., в том числе контактная работа обучающихся с преподавателем 80 ч., самостоятельная работа обучающихся 54 ч., промежуточная аттестация – 18 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)		Формы текущего контроля успеваемости, форма промежуточной
			контактная	Самостоятель-	

			Лекции	Семинар	Практические занятия	Лабораторные занятия	Контроль		аттестации *(по семестрам)*
1	Введение. Сущность организационного обеспечения информационной безопасности	4	2		4			4	Собеседование.
2	Организация работы по определению состава, засекречиванию и рассекречиванию (введению и снятию ограничения доступа) информации	4	2		4			4	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС)
3	Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности	4	2		4			4	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС)
4	Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. Работа с персоналом, имеющим допуск (доступ)	4	2		4			4	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС). Тест
5	Организация системы доступа к защищаемой информации (сведениям, документам, изделиям)	4	2		4			4	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС)
6	Организация пропускного и внутри объектового режимов	4	2		4			4	Собеседование, опрос «Мозговой штурм» или «Мозговая атака».
7	Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями	4	2		4			4	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС)
8	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам	4	2		4			4	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС).

									Контрольная работа
9	Организация защиты информации при приеме на объекте посетителей	4	4		4			4	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС)
10	Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности	4	4		4			4	Оценка выполнения задания в форме «Деловой игры»
11	Организационная защита конфиденциальных изделий (продукции) в процессе изготовления, хранения, транспортировки и утилизации	4	4		4			6	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС)
12	Организация внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности	4	4		4			8	Оценка выполнения практического задания по методу анализа конкретных ситуаций (АКС)
	Экзамен	4					18		Итоговая контрольная работа
	Итого		**32**		**48**		**18**	**54**	

3. Содержание дисциплины (модуля)

№	Наименование раздела дисциплины	Содержание
	Тема 1. Введение. Сущность организационного обеспечения информационной безопасности	Предмет и содержание курса, методы его изучения, источники и литература, контроль освоения. Понятия «организационное обеспечение информационной безопасности», «организационная защита информации» и «режим защиты информации». Определение указанных понятий по целям, функциям, структуре. Место организационной защиты информации в системе комплексной защиты информации.

		Принципы, методы и формы организационной защиты информации. Сущность организационных методов защиты информации. Соотношение организационных и правовых, организационных и технических методов защиты информации. Возможности перекрытия каналов утечки информации организационно-правовыми и организационно-техническими методами.
	Тема 2. Организация работы по определению состава, засекречиванию и рассекречиванию (введению и снятию ограничения доступа) информации	Принципы и порядок отнесения сведений к конфиденциальным. Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Присвоение и изменение грифа секретности документам и изделиям. Основания и порядок рассекречивания сведений (документов, изделий). Введение и снятие ограничения доступа к иной конфиденциальной информации. Перечни сведений, отнесенных к конфиденциальным. Полномочия по отнесению сведений к конфиденциальным и снятию грифа ограничения доступа.
	Тема 3. Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности	Основные цели, задачи, функции уполномоченных органов по ведению лицензионной деятельности. Порядок лицензирования деятельности предприятий (организаций) по проведению работ, связанных с использованием сведений, составляющих государственную тайну и иной конфиденциальной информации, созданием средств защиты информации, осуществлением

		мероприятий и (или) оказанием услуг по защите информации. Организация и проведение специальных экспертиз предприятий (организаций). Порядок рассмотрения заявлений о выдаче лицензии. Основания для выдачи (отказе в выдаче), приостановлении действия или аннулировании лицензии. Порядок проведения государственной аттестации руководителей предприятий. Осуществление контроля уполномоченными органами по ведению лицензионной деятельности.
	Тема 4. Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. Работа с персоналом, имеющим допуск (доступ)	Особенности подбора персонала на должности, связанные с конфиденциальной информацией. Состав документов, необходимых при подборе и приеме работников на должности, связанные с доступом к конфиденциальной информации. Понятия «номенклатуры должностей». Понятия «допуска». Формы допусков, их назначение и классификация. Порядок оформления допусков. Методы проверки кандидатов; особенности документирования трудовых отношений. Работа с персоналом, имеющим допуск и доступ к конфиденциальной информации.
	Тема 5. Организация системы доступа к защищаемой информации (сведениям, документам, изделиям)	Понятие «доступ к информации». Условия правомерного доступа. Задачи режима защиты информации, решаемые в процессе регулирования доступа. Цели и задачи разрешительной системы доступа. Организация работ по созданию разрешительной системы доступа. Положение о разрешительной системе доступа.

		Особенности доступа различных категорий персонала и командированных лиц. Обязанности лиц, допущенных к защищаемым сведениям.
	Тема 6. Организация пропускного и внутри объектового режимов	Организация охраны объектов информатизации и персонала. Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, прочие материальные и финансовые ценности. Виды и способы охраны. Понятие о рубежах охраны. Факторы выбора приемов и средств охраны. Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Понятие пропуска. Порядок оформления и выдачи пропусков. Бюро пропусков и контрольно-пропускные пункты, их оборудование и организация работы. Порядок прохода и проезда на территорию объекта. Порядок вывоза (выноса), ввоза (вывоза) материальных ценностей и документации. Понятие внутри объектового режима. Общие требования внутри объектового режима. Организационные требования к помещениям, в которых расположены защищаемые источники информации. Порядок доступа персонала в охраняемые помещения. Создание отдельных (выделенных) производственных зон (зон доступа) с самостоятельными системами организации и контроля доступа.
	Тема 7. Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями	Понятие режимных помещений, требования, предъявляемые к ним, особенности их оборудования. Порядок назначения комиссии для аттестации помещений. Документальное оформление после обследования помещений на пригодность.

		Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных документов и изделий. Порядок приема-сдачи под охрану режимных помещений. Назначение ответственных лиц, имеющих право вскрывать и опечатывать режимные помещения.
	Тема 8. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам	Общие требования к подготовке и проведению совещаний и переговоров по конфиденциальным вопросам. Обязанности лиц, участвующих в переговорах и ответственных за их проведение. Требования к помещениям, в которых проводятся совещания и переговоры. Подготовка программы проведения совещаний. Составление списков участников; порядок прохода приглашенных; документирование хода совещаний и их результатов; ведение записей; особенности использования технических средств документирования. Порядок реализации режимных мер в ходе подготовки и проведения совещаний и переговоров. Определение состава информации, используемой в ходе совещаний и переговоров. Документирование хода совещания (переговоров) и их результатов.
	Тема 9. Организация защиты информации при приеме на объекте посетителей	Требования режима защиты информации при приеме посетителей. Порядок доступа посетителей к конфиденциальной информации. Порядок пребывания посетителей на объекте. Организация контроля исполнения режимных требований в период пребывания посетителей. Особенности защитных мероприятий, осуществляемых при приеме различных категорий посетителей.

		Основания для приема на объекте иностранных граждан. Требования к программе приема иностранных граждан. Основные положения плана мероприятий по обеспечению режима конфиденциальности в период пребывания иностранных граждан на объекте. Требования к помещениям, в которых проводится прием представителей другой страны. Порядок ознакомления иностранных граждан со сведениями, составляющими конфиденциальную информацию. Особенности документирования в процессе переговоров. Порядок пересылки (передачи) документации этим лицам. Обязанности лиц, участвующих в работе с посетителями, в том числе с иностранными гражданами. Порядок отчетности о результатах работы.
	Тема 10. Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности	Понятия «издательская, рекламная и выставочная деятельность», виды, формы, особенности. Основные методы защиты информации в процессе этих видов деятельности и оценка эффективности защитных мероприятий. Особенности издательской деятельности. Общие требования режима защиты информации при опубликовании материалов в общедоступных изданиях (СМИ). Обеспечение прав личности на интеллектуальную собственность, при реализации мер по защите информации. Порядок создания и функционирования Экспертных комиссий, процедуры представления и рассмотрения материалов, предназначенных для открытого опубликования. Основания к принятию решений по результатам

		рассмотрения и оценки материалов. Документирование процессов рассмотрения материалов и принятия решений.
	Тема 11. Организационная защита конфиденциальных изделий (продукции) в процессе изготовления, хранения, транспортировки и утилизации	Разработка и проведение мероприятий по обеспечению режима конфиденциальности изделий (продукции). Организация учета. Основные требования при хранении, получении, транспортировке и уничтожении изделий. Документирование хода и результатов уничтожения изделий.
	Тема 12. Организация внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности	Понятие «внутреннее (служебное) расследование» по фактам нарушения режима конфиденциальности. Основания, цели и задачи внутреннего (служебного) расследования. Процедура внутреннего (служебного) расследования. Права и обязанности членов комиссии по проведению внутреннего (служебного) расследования. Документирование хода и результатов внутреннего (служебного) расследования. Взаимодействие с правоохранительными и судебными органами.

4. Образовательные технологии

При реализации рабочей программы дисциплины «Организационной обеспечение информационной безопасности» используются следующие образовательные технологии:

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Введение. Сущность организационного обеспечения информационной безопасности	Лекция 1.	Лекция. Дискуссия.
2	Организация работы по определению состава, засекречиванию и рассекречиванию (введению и	Лекция 2. Практическое занятие 1.	Лекция. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
	снятию ограничения доступа) информации		
3	Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности	Лекция 3. Практическое занятие 2.	Лекция. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
4	Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. Работа с персоналом, имеющим допуск (доступ)	Лекция 4. Практическое занятие 3.	Лекция с разбором конкретных ситуаций. Выполнение практического задания по методу анализа конкретных ситуаций (АКС). Выполнение теста.
5	Организация системы доступа к защищаемой информации (сведениям, документам, изделиям)	Лекция 5. Практическое занятие 4.	Лекция с разбором конкретных ситуаций. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
6	Организация пропускного и внутри объектового режимов	Лекция 6. Практическое занятие 5.	Лекция. Дискуссия. Устный опрос «Мозговой штурм» или «Мозговая атака»
7	Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями	Лекция 7. Практическое занятие 6.	Лекция с разбором конкретных ситуаций. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
8	Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам	Лекция 8. Практическое занятие 7.	Лекция с разбором конкретных ситуаций. Выполнение практического задания по методу анализа конкретных ситуаций (АКС). Выполнение контрольной работы.
9	Организация защиты информации при приеме на объекте посетителей	Лекция 9 Практическое занятие 8.	Лекция с разбором конкретных ситуаций. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
10	Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности	Лекция 10 Практическое занятие 9.	Лекция с разбором конкретных ситуаций. Выполнение задания в форме «Деловая игра».
11	Организационная защита конфиденциальных изделий (продукции) в процессе изготовления, хранения, транспортировки и утилизации	Лекция 11 Практическое занятие 10.	Лекция с разбором конкретных ситуаций. Выполнение практического задания по методу анализа конкретных ситуаций (АКС)
12	Организация внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности	Лекция 12 Практическое занятие 11.	Лекция с разбором конкретных ситуаций. Выполнение практического задания по методу анализа конкретных ситуаций (АКС).

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Система текущего и промежуточного контроля знаний по дисциплине «Организационное обеспечение информационной безопасности» предусматривает:

проведение текущего контроля знаний в устной форме (собеседовании, блиц-опрос), в письменном виде (выполнение практических ситуационных заданий), в письменном виде (выполнение контрольной работы, теста) и при помощи компьютерных технологий (тестирование);

проведение промежуточной аттестации (итоговой работы) в виде двух этапов: в форме решений ситуационных задач и форме тестирования.

По каждому виду и форме контроля предусмотрено следующее распределение баллов:

Форма контроля	Максимальное количество баллов	
	За одну работу	Всего
Текущий контроль: - выступления в ходе опроса по теме 6 - выполнение теста по теме 4 - выполнение практических заданий по темам 2, 3,4, 5, 7, 8 9, 10, 11, 12 - выполнение контрольной работы по темам 2-7 - выступления в ходе собеседования по теме 1	 5 баллов 5 баллов 4 баллов 5 баллов 5 баллов	 5 баллов 5 баллов 40 баллов 5 баллов 5 баллов
Промежуточная аттестация (итоговая работа)	40 баллов	
Итого за семестр (дисциплину):	100 баллов	

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	1-3	УК-2; ОПК-5; ОПК-6	План практического занятия
2.	4-5	УК-2; ОПК-5; ОПК-6	План практического занятия Контрольная работа
3.	6-7	УК-2; ОПК-5; ОПК-6	План практического занятия
4.	8-11	УК-2; ОПК-5; ОПК-6	План практического занятия
5.	12	УК-2; ОПК-5; ОПК-6	Тест

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
67-50/ D, E	зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине *(модулю)*

При оценивании ***текущего контроля*** знаний в устной форме (участие в дискуссии и собеседовании), выполнение письменной контрольной работы учитываются: полнота, логичность и доказательность выводов, глубина аргументации, а также правильность использования терминологии, знание нормативных документов и грамотное составление нормативно-методической документации по специальности и ***промежуточной аттестации*** (итоговой работы) в форме письменного теста учитываются: правильность ответов.

При оценивании заданий выполненных в письменном виде (практических заданий) учитываются правильность решения или степень соответствия этого решений поставленным задачам, аккуратность оформления работы, полнота ответов на

поставленные вопросы.

При проведении промежуточной аттестации (итоговой работы) при оценивании тестов (с помощью компьютерных технологий) учитывается количество правильных ответов (в соответствии с «ключами»).

Текущий контроль (вариант вопросов для компьютерного тестирования – один правильный ответ из четырех ответов) – проверка сформированности компетенций - УК-2; ОПК-5; ОПК-6

1. Перечень сведений, отнесенных к государственной тайне, утверждается...

2. Сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях должны иметь гриф…

3. При рассекречивании материалов государственных архивов направляют запросы…

4. Лицензии на разработку, производство, реализацию, приобретение специальных технических средств, предназначенных для негласного получения информации индивидуальными предпринимателями и юридическими лицами выдает..

5. Особое внимание на первых этапах проверки кандидата, принимаемого на должность, связанную с конфиденциальной информации должно уделяться анализу…

6. Дать определение «Допуск» - это…

7. В каком нормативном документе дано определение «допуск»…

8. Дать определение «Номенклатура должностей» - это…

9. Кем составляются списки на оформляемого лица и его близких родственников …

10. Материальные пропуска применяются для…

11. Образцы пропускных удостоверений утверждаются….

12. Выдачу пропускных документов осуществляет….

13. К хранилищам для документов с грифом ограничения относится….

14. Какое должно быть количество ключей от дверей в спецхранилища ….

15. Ответственным за проведение совещания по конфиденциальным вопросам является

16. Под работой с иностранными специалистами понимается….

18. Под разглашением следует понимать….

19. Срок определения грифа ограничения утраченных (разглашенных) документов (изделий) составляет….

20. Материалы по проведению служебному расследованию по факту утраты (разглашения) хранятся…..

21. Руководитель предприятия назначает комиссию для проведения служебного расследования с момента….

Промежуточная аттестация (экзамен) (примерные контрольные вопросы по курсу) – проверка сформированности компетенций - УК-2; ОПК-5; ОПК-6

1. Принципы, методы и способы организации защиты информации
2. Порядок установления и изменения грифа ограничения документов и изделий.
3. Порядок лицензирования деятельности предприятий (организаций) по проведению работ, связанных с использованием сведений, составляющих государственную тайну и иною конфиденциальной информации.
4. Порядок проведения государственной аттестации руководителей предприятий.
5. Порядок составления и прохождения номенклатуры должностей работников, подлежащих оформлению на допуск
6. Порядок оформления допуска к сведениям, имеющим гриф ограничения.
7. Формы допусков и их назначение.
8. Порядок оформления допуска граждан к государственной тайне.
9. Снижение формы и восстановление имевшегося допуска
10. Порядок учета и хранения справок о допуске и предписаний на выполнение заданий.
11. Документирование трудовых отношений при приеме на должность, связанную с работой с конфиденциальной информации.
12. Разрешительная система доступа и ее значение в системе защиты конфиденциальной информации.
13. Требования к составлению и оформлению Положения о разрешительной системе доступа к документам и сведениям предприятия.
14. Оформление доступа лиц к конфиденциальным документам государственных и негосударственных предприятий.
15. Организация доступа командированных лиц к конфиденциальной информации.
16. Организация и проведение приема иностранных граждан на предприятиях с различными формами собственности.
17. Основные требования к программе и плану мероприятий по приему иностранных граждан на режимном объекте.
18. Особенности приема сотрудников на работу
19. Критерии подбора персонала, процедуры подбора и документирования приема.
20. Процедура увольнения работников, связанных с конфиденциальной информацией и ее документирование.

21. Методы контроля за соблюдением персоналом правил работы с информацией ограниченного доступа.

22. Организация учета и хранения специзделий.

23. Организация пропускного режима на предприятии.

24. Виды охраняемых объектов. Назначение и задачи охраны объектов.

25. Порядок создания и функционирования контрольно-пропускных пунктов.

26. Понятие, виды пропусков и их оформление.

27. Шифры и вкладыши к пропускам и их назначение.

28. Порядок сдачи под охрану и снятия с охраны объектов и режимных помещений.

29. Назначение и задачи пропускного режима. Порядок организации доступа персонала в помещения различных категорий.

30. Понятие, задачи и структура внутри объектового режима.

31. Требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями.

32. Угрозы безопасности информации, задачи и направления ее защиты в процессе издательской, рекламной и выставочной деятельности.

33. Общие требования к отбору информации для оглашения, порядок отбора.

34. Порядок работы со средствами массовой информации. Виды рекламной деятельности, порядок отражения информации в рекламных изданиях.

35. Особенности и виды выставочной деятельности. Оформление разрешения на демонстрацию изделий и оглашение информации об изделиях, методы защиты информации.

36. Организационная защита конфиденциальной продукции (изделий) в процессе ее изготовления, хранения и транспортировки.

37. Организация внутреннего (служебного) расследования по фактам утраты или разглашения конфиденциальных документов и изделий.

38. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

2. Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

3. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

4. Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

5. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/

6. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

7. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

8. Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/

9. Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6387/

10. Постановление Правительства Российской Федерации от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_97474/

11. Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_54870/

Основная литература

1. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572

Дополнительная литература

1. Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль).

2. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова ; Южный федеральный университет. - Ростов-на-Дону - Таганрог : Издательство Южного федерального университета, 2017. - 76 с. - ISBN 978-5-9275-2501-0. - Текст: электронный. - URL: https://new.znanium.com/catalog/product/1021578

3. Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность).

4. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность).

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

КонсультантПлюс [Электронный ресурс]. – Электрон. дан. – М. : КонсультантПлюс, – Режим доступа : www.consultant.ru.

6.3.Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
2	Компьютерные справочные правовые системы Консультант Плюс,

	Гарант

7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Для проведения практических занятий и текущего контроля знания необходимы:

комплекты (на бумажном носителе и в электронной форме) заданий для работы и тесты;

комплекты раздаточного материала (на бумажном и электронном носителях по темам занятий).

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

- письменные задания выполняются на компьютере в письменной форме;

- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;

- в форме электронного документа;

- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;

- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;

- в форме электронного документа;

- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

- устройством для сканирования и чтения с камерой SARA CE;

- дисплеем Брайля PAC Mate 20;

- принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;

- акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемыми эргономическими партами СИ-1;

- компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Практическое занятие 1. (Тема 2). Организация работы по определению состава, засекречиванию и рассекречиванию (введению и снятию ограничения доступа) информации (2 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения принципы и порядок отнесения сведений к конфиденциальным. Провести анализ соотношения правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче указать действия со стороны администрации режимного предприятия по засекречиванию сведений, составляющих государственную тайну.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 2. «Организация работы по определению состава, засекречиванию и рассекречиванию (введению и снятию ограничения доступа) информации» и раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности».

Выполнение задания проходит в виде обсуждения и дискуссии, в ходе которых составляется необходимый документ, предоставляемый комиссии для засекречивания сведений (исходные данные предоставляет преподаватель дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Выделить сведения, подлежащие засекречиванию.

2. Указать действия исполнителя по указанному поручению, составив проект необходимого документа.

3. Определить правильность действий со стороны администрации режимного предприятия.

4. Используя лекционный материал перечислить функции комиссии, назначенной для анализа данных.

5. Составить исходный документ, оформив в соответствии с требованиями составления и оформления документа, имеющего гриф ограничения.

6. Отдельным разделом сделать выводы по работе с указанием правильности действий как исполнителя, так и администрации предприятия.

Контрольные вопросы:

1. Порядок установления и изменения степени секретности сведений, содержащихся в работах, документах и изделиях.
2. Порядок присвоения и изменения грифа секретности документам и изделиям.
3. Основания и порядок рассекречивания сведений (документов, изделий).
4. Порядок составления перечня сведений, отнесенных к конфиденциальным.
5. Порядок рассекречивания сведений, составляющих государственную тайну.

Список источников:

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/.

Список литературы:

Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль) – С.182-245.

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) - С.116-142.

Практическое занятие 2. (Тема 3). Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности (4 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения порядок лицензирования деятельности предприятий (организаций) по проведению работ, связанных с использованием сведений, составляющих государственную тайну и иной конфиденциальной информации.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче указать технологические действия со стороны администрации предприятия, желающего заниматься деятельностью в области информационной безопасности, подпадающую под лицензирование.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 3. «Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности», законодательные, нормативные документы, а также раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности». Выполнение задания проходит в виде подготовки необходимых документов для подачи соискателем лицензии в уполномоченный орган. (Исходные данные предоставляются преподавателем дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Выделить виды деятельности, подлежащих лицензированию в области защиты информации, сославшись на законодательные документы.

2. Подготовить перечень необходимых документов для подачи соискателем лицензии в уполномоченный орган.

3. Указать действия исполнителей по указанному поручению и определить их должностной состав.

4. Используя лекционный материал перечислить типичные ошибки, возникающие при подаче документов соискателем лицензии в уполномоченный орган, что может явиться основания для отказе в выдаче, приостановлении действия или аннулировании лицензии.

5. Рассмотреть организацию и проведение специальных экспертиз предприятий (организаций) на примере ситуационной задачи.

6. Технологично рассмотреть порядок проведения государственной аттестации руководителей предприятий.

Контрольные вопросы:

1. Каковы основные цели, задачи, функции уполномоченных органов по ведению лицензионной деятельности?

2. Каков порядок лицензирования деятельности предприятий (организаций) по проведению работ, связанных с использованием сведений, составляющих государственную тайну и иной конфиденциальной информации?

3. Каков порядок лицензирования деятельности предприятий (организаций) по проведению работ, связанных с созданием средств защиты информации, осуществлением мероприятий и (или) оказанием услуг по защите информации?

4. Каков порядок осуществления контроля уполномоченными органами по ведению лицензионной деятельности?

Список источников:

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6387/.

Список основной литературы:

Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572

Список дополнительной литературы:

Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль) – С.477-519.

Правовое обеспечение информационной безопасности : учебник / [авт.-ред. В. А. Минаев и др.]. - Изд. 2-е, расшир. и доп. - М. : Маросейка, 2008. - 368 с. - (Серия "Информатика и информационная безопасность") – С.157-174.

Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы / А. А. Стрельцов ; Московский гос. ун-т им. М. В. Ломоносова, Ин-т проблем информ. безопасности. - Минск : Беллітфонд, 2005. - 303 с. - (Библиотека журнала "УЗИ" кн. 3) – 304 с.

Практическое занятие 3. (Тема 4). Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. Работа с персоналом, имеющим допуск (доступ) (4 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения особенности подбора персонала на должности, связанные с конфиденциальной информацией, методы проверки кандидатов; особенности документирования трудовых отношений.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче подготовить и оформить в установленном порядке допуск к сведениям, составляющих государственную тайну.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 4. «Оформление допуска граждан к государственной тайне», законодательные, нормативные документы, а также и раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности». Выполнение задания проходит в виде подготовки необходимых документов для отправки на согласование в орган госбезопасности. (Исходные данные предоставляются преподавателем дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Определить форму допуска необходимую для оформления.

2. Выбрать из предложенных унифицированных форм нужные для заполнения.

3. Указать последовательность действий кандидата на вакантную должность и исполнителя от организации по указанному поручению.

4. Составить перечень оснований для отказа в получении допуска к государственной тайне.

5. Составить все необходимые документы в соответствии с требованиями по их оформлению и подготовить их на отправку (как исходящую корреспонденцию с грифом ограничения).

Контрольные вопросы:

1. Каков состав документов, необходимых при подборе и приеме работников на должности, связанные с доступом к информации ограниченного распространения?

2. Каков порядок составления и оформления «номенклатуры должностей»?

3. Формы допусков, их назначение и классификация. Порядок оформления допусков.

4. Особенности работы с персоналом, имеющим допуск и доступ к информации ограниченного распространения.

Список источников:

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Постановление Правительства Российской Федерации от 06.02.2010 № 63 «Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_97474/.

Список основной литературы:

Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572

Список дополнительной литературы:

Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль) – С.477-519.

Правовое обеспечение информационной безопасности : учебник / [авт.-ред. В. А. Минаев и др.]. - Изд. 2-е, расшир. и доп. - М. : Маросейка, 2008. - 368 с. - (Серия "Информатика и информационная безопасность") – С.157-174.

Практическое занятие 4. (Тема 5). Организация системы доступа к защищаемой информации (сведениям, документам, изделиям) (2 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения условия правомерного доступа к информации ограниченного доступа работников и задачи режима защиты информации, решаемые в процессе регулирования доступа.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче подготовить и оформить в установленном порядке нормативно-методический документ – Положение о разрешительной системе доступа.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 5. «Организация системы доступа к защищаемой информации (сведениям, документам, изделиям)», законодательные, нормативные документы, а также и раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности». Выполнение задания проходит в виде подготовки проекта документа для последующего внедрения в деятельность предприятия (организации). (Исходные данные предоставляются преподавателем дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Определить структуру документа.

2. Указать последовательность действий администрации предприятия и исполнителей (членов комиссии) при разработке проекта документа.

3. Провести анализ предложенных сведений, доступ к которым требуется исполнителям.

5. Составить проект документа – Положение о разрешительной системе доступа.

6. Разработать учетные формы для реализации доступа.

7. Предложить варианты процедуры ознакомления с информацией, имеющей гриф ограничения с фиксацией такого факта в разрешительных документах предприятия.

Контрольные вопросы:

1. Понятие «доступ к информации». В каком законодательном документе дано это определение?

2. Каковы цели и задачи разрешительной системы доступа?

3. Какова организация работ по созданию разрешительной системы доступа?

4. Особенности доступа различных категорий персонала и командированных лиц.

5. Обязанности лиц, допущенных к защищаемым сведениям.

Список источников:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_54870/

Список дополнительной литературы:

Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." /

П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль) – С.561-571.

Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.58-75.

Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы / А. А. Стрельцов ; Московский гос. ун-т им. М. В. Ломоносова, Ин-т проблем информ. безопасности. - Минск : Беллітфонд, 2005. - 303 с. - (Библиотека журнала "УЗИ" кн. 3) – 304 с.

Практическое занятие 5. (Тема 6). Организация пропускного и внутри объектового режимов (4 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть порядок организации пропускного и внутри объектовых режимов на предприятии. Порядок оформления и выдачи необходимых документов, обеспечивающих вышеуказанные режимы. Сформировать подходы к разработке локальных нормативно-методических документов предприятия (организации), регламентирующих порядок пропускного и внутри объектовых режимов.

Порядок выполнения работы:

В ходе выполнения работы используется имитационный игровой метод и технология - «Мозговой штурм» или «Мозговая атака», которые направлены на стимулирования творческой активности, позволяющие найти решение сложной проблемы внутри предложенного объекта. Предложить решения по организации пропускного и внутри объектового режимов с предложениями по разработке локальных документов предприятия. В связи с тем, что предложенная ситуационная задача относится к объекту, в обращении которого находится сведения конфиденциального характера, студентам предлагается высказать разные точки зрения в области организации пропускного и внутри объектового режимов при этом не высказывать негативную оценку или критику в адрес любой идеи, возникшей в ходе обсуждения. Постараться использовать свой творческий потенциал, знания и умения, полученные в ходе обучения и высказать как можно больше вариантов управленческого решения.

Процедура проведения занятий по методу «мозгового штурма» состоит из следующих этапов:

1. Формулирование проблемы, которую необходимо решить, обоснование задачи для поиска решения. Определение условий групповой работы, знакомство с правилами поведения в процессе «мозгового штурма».

Таким образом, преподавателем предлагается студентам разбиться на две группы (первая группа будет состоять из несколько подгрупп по 5-7 человек): на тех, кто должен предложить новые варианты решения ситуационной задачи, т.е. «генераторов идей», и «членов экспертной комиссии», которые будут обрабатывать предложенные материалы - «критиков». Задача «генераторов» состоит в том, чтобы набросать как можно больше предложений, идей относительно возможностей решения ситуации. На практическом примере, описанном в ситуационной задаче предложить решения по подготовке и оформлению в установленном порядке нормативно-методических документов – Положение о пропускном режиме и Положение о внутри объектовом режиме.

В ходе выполнения работы первой группе - «генераторов» необходимо использовать лекционный материал по Теме 6. «Организация пропускного и внутри объектового режимов», а также нормативные документы. Итогом выполнения задания будут являться решения в подготовке проектов документов для последующего внедрения в деятельность объекта (предприятия, организации). (Исходные данные предоставляются преподавателем дисциплины).

2. Разминочная сессия, т.е. упражнения на быстрый поиск ответов на вопросы. Задача этого этапа – помочь участникам максимально освободиться от воздействия психологических барьеров (неловкости, стеснительности, замкнутости, скованности и пр.). Для этого преподаватель проводит устный опрос по Теме 6. «Организация пропускного и внутри объектового режимов», задавая конкретные практические вопросы.

3. Рабочая сессия, т.е. сам «штурм» поставленной проблемы. Еще раз уточняются задачи, напоминаются правила поведения в ходе работы. Генерирование идей начинается по сигналу руководителя во всех рабочих группах. К каждой группе прикрепляется один эксперт, в задачу которого входит фиксирование на доске или большом листе бумаге все выдвигаемые идеи.

Для выполнения работы первой группе «генераторов» и второй группе «критиков» необходимо:

- Ознакомиться с ситуационной задачей. Определить организационно-правовую форму и структуру предприятия.
- В ходе анализа ситуации определить необходимость создания нормативно-методических документов предприятия.

- Указать последовательность действий администрации предприятия и исполнителей в ходе разработке проектов документов.
- Провести анализ деятельности предприятия в соответствии с объемом сведений, ограниченного доступа. Определить структуру (по разделам) локальных документов предприятия.

Для выполнения работы первой группе «генераторов» необходимо:

- Дать предложения по составлению проектов документов – Положение о пропускном режиме и Положение о внутри объектовом режиме. Предложенные решения, идеи и варианты проектов документов могут быть любыми, неаргументированными, с долей творческого подхода к выполнению задания.

4. Экспертиза – оценка собранных идей и отбор лучших из них в группе «критиков» на основе разработанных ими критериев. Рабочие группы в это время отдыхают.

Для выполнения работы второй группе «критиков» необходимо:

- Обработать предложенные материалы – решения по включению в проекты документов (в Положение о пропускном режиме и в Положение о внутри объектовом режиме).
- Выполняя роль «членов экспертной комиссии» проанализировать решения, идеи и варианты проектов документов на предмет соответствия законодательной и нормативной базы, выявить ошибки, сделать замечания и/или конструктивные предложения. Выбрать из предложенных решений, идей и вариантов проектов документов лучшие.
- Указать правильное управленческое решение по вводу в действие вышеуказанных документов.
- Указать решение по реализации действия по ознакомлению работников предприятия с нормативными документами.

5. Подведение итогов - общее обсуждение результатов работы групп, представление лучших идей, их обоснование и публичная защита. Принятие общего группового решения, его фиксация.

Любой участник на каждом этапе «мозговой атаки» имеет возможность для высказывания в строго лимитированное время, обычно в пределах от одной до трех минут.

Ведущий «мозговую атаку» не имеет права комментировать или оценивать высказывания участников. Но может прервать участника, если он высказывается не по

теме или исчерпал лимит времени, а также в целях уточнения сути высказанных предложений.

Контрольные вопросы:

1. Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы, прочие материальные и финансовые ценности.

2. Каков Порядок оформления и выдачи пропусков?

3. Каков порядок прохода и проезда на территорию объекта? Порядок вывоза (выноса), ввоза (вывоза) материальных ценностей и документации?

4. Каковы общие требования внутри объектового режима?

5. Каков порядок создания отдельных (выделенных) производственных зон (зон доступа) с самостоятельными системами организации и контроля доступа?

Список источников:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

Список дополнительной литературы:

Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.75-96.

Практическое занятие 6. (Тема 7). Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями (2 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения порядок назначения комиссии для аттестации помещений. Документальное оформление после обследования помещений, предназначенных для хранения конфиденциальных документов и изделий на пригодность.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче подготовить и оформить в установленном порядке все документы по назначению комиссии для аттестации помещений, обследованию на предмет пригодности данного помещения для работы и хранению конфиденциальных документов и изделий.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 7. «Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями», нормативные документы, а также и раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности». Выполнение задания проходит в виде подготовки проектов документов. (Исходные данные предоставляются преподавателем дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Определить категории предложенных помещений.

2. Подготовить проект документа (определив его вид) по назначению комиссии для аттестации помещений.

3. Указать последовательность действий администрации предприятия и исполнителей в ходе разработке проекта документов.

4. Провести обследование конкретных помещений (характеристики помещений даны в ситуационной задаче).

5. Составить паспорта помещений с указанием всех технических средств, находящихся в них.

6. Определить отличия помещений, предназначенных для работы с конфиденциальными сведениями и помещений для хранения конфиденциальных документов и изделий.

7. Ввести в действие вышеуказанные документы.

Контрольные вопросы:

1. Дать понятие «режимных помещений».

2. Каковы требования, предъявляемые к режимным помещениям, особенности их оборудования?

3. Каково оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных документов и изделий?

4. Порядок назначения ответственных лиц, имеющих право вскрывать и опечатывать режимные помещения.

Список источников:

Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Список основной литературы:

Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572

Список дополнительной литературы:

Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.96-111.

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.207-224.

Практическое занятие 7. (Тема 8). Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам (2 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения порядок подготовки и проведения совещаний и переговоров по конфиденциальным вопросам. Сформировать навыки составления необходимых документов по вопросам подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче подготовить и оформить в установленном порядке все документы по организации подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 8. «Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам», нормативные документы, а также раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности». Выполнение задания проходит в виде подготовки проектов документов. (Исходные данные предоставляются преподавателем дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Определить порядок действий исполнителей.

2. Определить обязанности лиц, участвующих в переговорах и их ответственность за данное поручение.

3. Указать последовательность действий администрации предприятия и исполнителей в ходе организации подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.

4. Выделить отличия в организации подготовки внутренних (служебных) совещаний и проведения переговоров с приглашением сторонних представителей.

5. Подготовить проекты документов (определив их виды) по указанному поручению.

6. Ввести в действие вышеуказанные документы, указав места их дальнейшего хранения.

Контрольные вопросы:

1. Каковы требования к помещениям, в которых проводятся совещания и переговоры?

2. Каковы требования, предъявляемые к составлению списков участников; порядку прохода приглашенных; документированию хода совещаний и их результатов; ведению записей.

3. Каковы особенности использования технических средств документирования?

3. Каков порядок определения состава информации, используемой в ходе совещаний и переговоров?

4. Порядок документирования хода совещания (переговоров) и их результатов.

Список источников:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Список основной литературы:

Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572

Список дополнительной литературы:

Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.119-127.

Практическое занятие 8. (Тема 9). Организация защиты информации при приеме на объекте посетителей (2 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения порядок доступа посетителей к конфиденциальной информации. Сформировать навыки по организации контроля исполнения режимных требований в период пребывания посетителей.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче подготовить и оформить в установленном порядке все документы по организации порядка доступа посетителей к конфиденциальной информации (с учетом особенностей посетителей, которые не являются гражданами Российской Федерации).

В ходе выполнения работы необходимо использовать лекционный материал по Теме 9. «Организация защиты информации при приеме на объекте посетителей», нормативные документы, а также раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности».. Выполнение задания проходит в виде подготовки проектов документов. (Исходные данные предоставляются преподавателем дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Определить основания для приема на объекте иностранных граждан.

2. Определить обязанности лиц, участвующих в приеме на объекте посетителей.

3. Указать последовательность действий администрации предприятия и исполнителей в ходе организации подготовки приема на объект посетителей.

4. Определить особенности защитных мероприятий, осуществляемых при приеме различных категорий посетителей.

5. Подготовить проекты документов по указанному поручению: Программу приема иностранных граждан; План мероприятий по обеспечению режима конфиденциальности в период пребывания иностранных граждан на объекте.

6. Определить требования к помещениям, в которых будет проводиться прием представителей другой страны.

7. Разработать порядок и документ по ознакомлению иностранных граждан со сведениями, составляющими конфиденциальную информацию.

6. Провести встречу и в соответствии с ситуационной задачей оформить все необходимые документы в процессе проведения переговоров.

7. Составить отчет о результатах работы и сдать его ответственному лицу за организацию и проведение указанного совещания.

Контрольные вопросы:

1. Каковы требования режима защиты информации при приеме посетителей?

2. Каков порядок пребывания посетителей на объекте?

3. Каковы требования к программе приема иностранных граждан?

4. Каковы особенности документирования в процессе переговоров. Порядок пересылки (передачи) документации этим лицам?

5. Каковы обязанности лиц, участвующих в работе с посетителями, в том числе с иностранными гражданами?

Список источников:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Список основной литературы:

Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572

Список дополнительной литературы:

Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.119-127.

Мосягина Е. Конфиденциальность и защита информации при работе с зарубежными партнерами / Е. Мосягина, Г. Шевцова ; под ред. В. И. Ярочкина. - М. : Паруса, 1999. - 99 с. -С.6-99.

Практическое занятие 9. (Тема 10). Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности (4 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения в форме «Деловой игры» методы защиты информации в процессе издательской, рекламной и выставочной деятельность и оценить эффективность защитных мероприятий. Также проявить имеющиеся знания, показать умение в команде пользоваться ими, получить навыки уяснения комплексных проблем и выработки подходов к их решению.

«Деловая игра» по Теме 10. содержит игровую и учебную задачи. Игровая задача – выполнение играющим определенной профессиональной деятельности в области обеспечения информационной безопасности. Учебная задача – овладение знаниями и умениями в области организации защиты при осуществлении издательской, рекламной и выставочной деятельности.

Порядок проведения «Деловой игры»:

Деловая игра состоит из некоторых последовательных шагов:

1. Преподавателем доводиться проблемная задача до участников игры.

На практическом примере, описанном в ситуационной задаче, которое раздается участникам игры необходимо подготовить и оформить в установленном порядке все документы по порядку создания и функционирования Экспертных комиссий. Провести процедуру представления и рассмотрения материалов, предназначенных для открытого опубликования. В Экспертном заключении указать основания к принятию решения по результатам рассмотрения и оценки материалов.

Распечатанный текст ситуационной задачи предоставляется каждому участнику игры. Условия игры в ситуационной задачи принимаются, что и в реальной жизни при решении сходных задач.

2. Группа разбивается на три команды. «Первая» команда – исполнители документа. «Вторая» команда – эксперты. «Третья» команда – администрация предприятия.

3. Работа команд.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 10. «Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности», а также законодательные и нормативные документы, выдержки из которых предоставляются в виде раздаточного материала. (Исходные данные ситуационной задачи предоставляются преподавателем дисциплины).

Для выполнения задания «Первой» команде необходимо:

- Ознакомиться с ситуационной задачей и раздаточным материалом.
- Подготовить проект документа для открытого опубликования.

- Предоставить проект документа для открытого опубликования «Второй» команде – экспертам для анализа на предмет наличия/отсутствия сведений, составляющих конфиденциальную информацию.

Для выполнения задания «Второй» команде необходимо:

- Ознакомиться с ситуационной задачей и раздаточным материалом.
- Провести аналитическую работу на предмет наличия в подготовленном проекте документа для открытого опубликования сведений, составляющих конфиденциальную информацию.
- Определить обязанности лиц, участвующих в анализе исходного материала.
- Выделить сведения (на основании Перечня сведений, составляющих коммерческую тайну предприятия) распространение которых недопустимо.
- Подготовить проект заключения экспертной комиссии о возможности/не возможности опубликования представленного материала в открытых источниках.

Для выполнения задания «Третьей» команде необходимо:

- Ознакомиться с ситуационной задачей и раздаточным материалом.
- Подготовить и оформить в установленном порядке все документы по порядку создания и функционирования Экспертных комиссий.
- Определить последовательность действий администрации предприятия, исполнителя и экспертов в ходе рассмотрения материала для открытого опубликования и в случае необходимости выявить нарушения.
- Получить от «Второй» команды подготовленный проект заключения экспертной комиссии о возможности/не возможности опубликования представленного материала в открытых источниках.
- Провести анализ исходного документа и в случае положительного решения проставить в необходимой очередности все необходимые отметки на документе (реквизиты «Подпись», «Согласовано», «Утверждаю»).

4. Подведение итога.

Каждая команда должна подготовить короткий (до 10 минут) устный доклад о своих подходах и методах решения поставленных задач и о самом решении. Доклад составляется в произвольной форме игрового результата.

После заслушивания всех докладов от трех команд производится их оценка самим преподавателем, дается сравнительная характеристика всех трех подходов и подводится итог проведенной работы каждой из трех команд.

Контрольные вопросы:

1. Каковы основные методы защиты информации в процессе этих видов деятельности и оценка эффективности защитных мероприятий?

2. Каковы общие требования режима защиты информации при опубликовании материалов в общедоступных изданиях (СМИ)?

3. Какие законодательные нормативные документы регламентируют обеспечение прав личности на интеллектуальную собственность, при реализации мер по защите информации?

4. Каковы Основания к принятию решений по результатам рассмотрения и оценки материалов?

5. Какова процедура документирования процессов рассмотрения материалов и принятия решений по открытому опубликованию?

Список источников:

Федеральный закон от 13.03.2006 N 38-ФЗ «О рекламе» // Собр. законодательства Рос. Федерации. – 2006. http://www.consultant.ru/document/cons_doc_LAW_58968/.

Список дополнительной литературы:

Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.127-139.

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.93-116.

Правовое обеспечение информационной безопасности : учебник / [авт.-ред. В. А. Минаев и др.]. - Изд. 2-е, расшир. и доп. - М. : Маросейка, 2008. - 368 с. - (Серия "Информатика и информационная безопасность") – С.195-223.

Городов О. А. Информационное право : учебник / О. А. Городов. - М. : Проспект : ТК Велби, 2009. - 242 с. - С.157-199.

Сергеев А. П. Право интеллектуальной собственности в Российской Федерации : учебник для студентов вузов, обучающихся по специальности 021100 "Юриспруденция" / А. П. Сергеев. - Изд. 2-е, перераб. и доп. - М. : Проспект, 2004. - 750 с. – 752 с.

Практическое занятие 10. (Тема 11). Организационная защита конфиденциальных изделий (продукции) в процессе изготовления, хранения, транспортировки и утилизации (2 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки технологические составляющие разработки изделий (продукции) и проведение мероприятий по обеспечению режима конфиденциальности.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче разработать технологическую цепочку полного цикла от разработки изделия (продукции), хранения, получении, транспортировки и уничтожения. Указав все учетные регистрационные формы.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 11. «Организационная защита конфиденциальных изделий (продукции) в процессе изготовления, хранения, транспортировки и утилизации», нормативные документы, а также раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности». Выполнение задания проходит в виде проведения регистрации по учетным формам по каждому технологическому циклу. (Исходные данные предоставляются преподавателем дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Проанализировать материал, выделив технологические этапы разработки изделия (продукции), имеющих гриф ограничения.

2. Определить обязанности лиц, участвующих в разработке изделия (продукции), имеющих гриф ограничения.

3. Указать последовательность действий исполнителя в ходе разработке изделия (продукции), имеющих гриф ограничения.

4. Заполнить все необходимые учетные регистрационные формы по каждому технологическому циклу.

5. Определить круг должностных лиц, включенных в состав комиссии по отбору изделия (продукции) на уничтожение.

6. Подготовить проект акта утилизации изделия (продукции), имеющих гриф ограничения.

Контрольные вопросы:

1. Порядок разработки мероприятий по обеспечению режима конфиденциальности изделий (продукции).

2. Основные мероприятий по обеспечению режима конфиденциальности при хранении изделий (продукции).

3. Каков порядок организации учета изделий (продукции), имеющих гриф ограничения?

3. Основные требования при хранении, получении, транспортировке и уничтожении изделий.

4. Приведите основные требования при хранении, получении, транспортировке и уничтожении изделий (продукции).

5. Каков порядок документирования хода и результатов уничтожения изделий?

Список дополнительной литературы:

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.116-126.

Правовое обеспечение информационной безопасности : учебник / [авт.-ред. В. А. Минаев и др.]. - Изд. 2-е, расшир. и доп. - М. : Маросейка, 2008. - 368 с. - (Серия "Информатика и информационная безопасность") – С.195-223.

Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М. : Проспект : ТК Велби, 2008. - 333 с. – С.29-50.

Практическое занятие 11. (Тема 12). Организация внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности (4 часа) - *проверка сформированности компетенций* - УК-2; ОПК-5; ОПК-6

Цель работы: рассмотреть с практической точки зрения технологию проведения внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности и подготовить все необходимые документы.

Порядок выполнения работы:

На практическом примере, описанном в ситуационной задаче, выполняя роль члена комиссии по проведению служебного расследования по фактам нарушения режима конфиденциальности установить виновных лиц и составить проект заключения по данному факту.

В ходе выполнения работы необходимо использовать лекционный материал по Теме 12. «Организация внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности», законодательные, нормативные документы, а также раздаточный материал «Сборник ситуационных задач по дисциплине «Организационное и правовое обеспечение информационной безопасности» Часть II. «Организационное обеспечение информационной безопасности».. Выполнение задания проходит в виде составления проекта документа. (Исходные данные предоставляются преподавателем дисциплины).

Для выполнения практической работы необходимо:

1. Ознакомиться с ситуационной задачей. Выявить нарушения в режиме конфиденциальности.

2. Определить порядок проведения служебного расследования по фактам нарушения режима конфиденциальности.

3. Указать права и обязанности членов комиссии по проведению внутреннего (служебного) расследования.

4. Указать последовательность действий администрации в ходе проведения внутреннего (служебного) расследования.

5. Определить виновных лиц.

6. Подготовить проект заключения по факту разглашения/утраты/нарушения режима конфиденциальности.

Контрольные вопросы:

1. Каковы основания, цели и задачи внутреннего (служебного) расследования?

2. Какова процедура внутреннего (служебного) расследования?

3. Порядок документирования хода и результатов внутреннего (служебного) расследования.

4. Документирование хода и результатов внутреннего (служебного) расследования.

5. Каковы права и обязанности членов комиссии по проведению внутреннего (служебного) расследования?

6. Каков порядок взаимодействия с правоохранительными и судебными органами?

Список источников:

Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/.

Кодекс об административных правонарушениях от 30.12.2001 г. № 195-ФЗ // Собр. законодательства Рос.Федерации. – 2002. - http://www.consultant.ru/document/cons_doc_LAW_34661/

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Собр. законодательства Рос. Федерации. – 2002. – http://www.consultant.ru/document/cons_doc_LAW_34683/.

Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне”, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/

Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/

Список дополнительной литературы:

Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.167-173

Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.116-126.

Городов О. А. Информационное право : учебник / О. А. Городов. - М. : Проспект : ТК Велби, 2009. - 242 с. - С.288-302.

10. Методические рекомендации по организации самостоятельной работы

Трудоемкость освоения дисциплины «Организационное обеспечение информационной безопасности» составляет 152 часов, из них 54 часов отведены на самостоятельную работу студента (СР).

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
Подготовка к лекции и собеседованию Тема 1.Сущность организационного обеспечения информационной безопасности	Понятия «организационное обеспечение информационной безопасности», «организационная защита информации» и «режим защиты информации». Определение указанных понятий по целям, функциям, структуре. Место организационной защиты информации в системе комплексной защиты информации	8	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_108546/. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/. Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне” Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.5-24. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям:

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			075200 - Компьютерная безопасность, 075500 - Комплексное обеспечение информ. безопасности автоматизированных систем, 075600 - Информ. безопасность телекоммуникационных систем / [С. Я. Казанцев и др.] ; под ред. С. Я. Казанцева. - М. : Академия, 2005. - 238 с. - (Высшее профессиональное образование. Информационная безопасность) – С.7-28.
Подготовка к практическому занятию Тема 2. Организация работы по определению состава, засекречиванию и рассекречиванию (введению и снятию ограничения доступа) информации	Принципы и порядок отнесения сведений к конфиденциальным. Установление и изменение степени секретности сведений. Присвоение и изменение грифа ограничения документам и изделиям. Основания и порядок рассекречивания сведений (документов, изделий).	8	Проанализировать материал из законодательных, нормативных документов, учебников Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне” Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/. Указ Президента Российской Федерации от 06.03.97 № 188 “Об утверждении перечня сведений конфиденциального характера” Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_13532/ Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль) – С.7-35. Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А.

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) - С.116-142. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.34-46. Основы организационного обеспечения информационной безопасности объектов информатизации : учеб. пособие по специальностям в обл. информ. безопасности / С. Н. Семкин [и др.]. - М. : Гелиос АРВ, 2005. - 185 с. Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы / А. А. Стрельцов ; Московский гос. ун-т им. М. В. Ломоносова, Ин-т проблем информ. безопасности. - Минск : Беллітфонд, 2005. - 303 с. - (Библиотека журнала "УЗИ" кн. 3)
Подготовка к практическому занятию Тема 3. Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности	Основные цели, задачи, функции уполномоченных органов по ведению лицензионной деятельности. Порядок лицензирования деятельности предприятий (организаций) по проведению работ, связанных с использованием сведений, составляющих государственную тайну и иной конфиденциальной информации. Осуществление контроля уполномоченными органами по ведению лицензионной деятельности.	8	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_113658/ Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/. Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6387/. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572 Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль) – С.477-519. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям: 075200 - Компьютерная безопасность, 075500 - Комплексное обеспечение информ. безопасности автоматизированных систем, 075600 - Информ. безопасность телекоммуникационных систем / [С. Я. Казанцев и др.] ; под ред. С. Я. Казанцева. - М. : Академия, 2005. - 238 с. - (Высшее профессиональное образование. Информационная безопасность) – С.157-174. Основы организационного обеспечения информационной безопасности объектов

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			информатизации : учеб. пособие по специальностям в обл. информ. безопасности / С. Н. Семкин [и др.]. - М. : Гелиос АРВ, 2005. - 185 с. Стрельцов А. А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы / А. А. Стрельцов ; Московский гос. ун-т им. М. В. Ломоносова, Ин-т проблем информ. безопасности. - Минск : Беллітфонд, 2005. - 303 с. - (Библиотека журнала "УЗИ" кн. 3).
Подготовка к лекции и тесту по Теме 4. Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. Работа с персоналом, имеющим допуск (доступ)	Сравнить понятия «допуск» и «доступ». Особенности подбора персонала на должности, связанные с конфиденциальной информацией. Определить состав документов, необходимых при подборе и приеме работников на должности, связанные с доступом к конфиденциальной информации. Рассмотреть порядок оформления допусков. Работа с персоналом, имеющим допуск и доступ к конфиденциальной информации.	12	Проанализировать материал из законодательных, нормативных документов, учебников: Закон Российской Федерации от 21.07.93 № 5485-1 “О государственной тайне” Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/ Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/. Постановление Правительства Российской Федерации от 03.11.94 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» Режим доступа: http://www.consultant.ru/document/co

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			ns_doc_LAW_54870/. Государственная тайна и ее защита в Российской Федерации : учеб. пособие для студентов вузов, обучающихся по направлению подгот. 220100 - "Систем. анализ и упр." / П. П. Аникин [и др.] ; под общ. ред.: М. А. Вуса и А. В. Федорова ; Ассоц. Юрид. центр, С.-Петерб. ин-т информатики и автоматизации РАН, Междунар. комис. по защите гос. тайны. - 3-е изд., испр. и доп. - СПб. : Юрид. центр Пресс, 2007. - 745 с. - (Государственное управление и государственный надзор и контроль) – С.561-571. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.58-75. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям: 075200 - Компьютерная безопасность, 075500 - Комплексное обеспечение информ. безопасности автоматизированных систем, 075600 - Информ. безопасность телекоммуникационных систем / [С. Я. Казанцев и др.] ; под ред. С. Я. Казанцева. - М. : Академия, 2005. - 238 с. - (Высшее профессиональное образование. Информационная безопасность) – С.35-85.
Подготовка к лекции и к практическому занятию по Теме 5. Организация системы доступа к защищаемой	Понятие «доступ к информации». Условия правомерного доступа. Задачи режима защиты информации, решаемые в процессе регулирования доступа.	8	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности» Режим доступа: http://www.consultant.ru/document/co

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
информации (сведениям, документам, изделиям)	Организация работ по созданию разрешительной системы доступа.		ns_doc_LAW_108546/. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.75-96. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям: 075200 - Компьютерная безопасность, 075500 - Комплексное обеспечение информ. безопасности автоматизированных систем, 075600 - Информ. безопасность телекоммуникационных систем / [С. Я. Казанцев и др.] ; под ред. С. Я. Казанцева. - М. : Академия, 2005. - 238 с. - (Высшее профессиональное образование. Информационная безопасность) – С.35-85. Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М. : Проспект : ТК Велби, 2008. - 333 с. Ярочкин В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. - [4-е изд.]. - М. : Акад. проект, 2006. - 542 с. - (Gaudeamus).
Подготовка к устному опросу по Теме 6. Организация	Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы,	12	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 27.12.2002

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
пропускного и внутри объектового режимов	прочие материальные и финансовые ценности. Виды и способы охраны. Понятие о рубежах охраны. Создание отдельных (выделенных) производственных зон (зон доступа) с самостоятельными системами организации и контроля доступа.		№ 184-ФЗ «О техническом регулировании» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_40241/. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.96-111. Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.207-224. Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М. : Проспект : ТК Велби, 2008. - 333 с. Ярочкин В. И. Информационная безопасность : учебник для вузов / В. И. Ярочкин. - [4-е изд.]. - М. : Акад. проект, 2006. - 542 с. - (Gaudeamus).
Подготовка к практическому занятию Тема 7. Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиям	Понятие режимных помещений, требования, предъявляемые к ним, особенности их оборудования. Оборудование специальных хранилищ, сейфов и металлических шкафов, предназначенных для хранения конфиденциальных документов и изделий. Порядок приема-сдачи под охрану режимных помещений.	12	Проанализировать материал из учебников: Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.96-111. Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А.

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.207-224. Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М. : Проспект : ТК Велби, 2008. - 333 с.
Подготовка к лекции и контрольной работе по Теме 8. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам	Общие требования к подготовке и проведению совещаний и переговоров по конфиденциальным вопросам. Обязанности лиц, участвующих в переговорах и ответственных за их проведение. Определение состава информации, используемой в ходе совещаний и переговоров.	12	Проанализировать материал из учебников: Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572 Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.119-127. Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М. : Проспект : ТК Велби, 2008. - 333 с. – С.193-201.
Подготовка к лекции Тема 9. Организация защиты информации при приеме на объекте посетителей	Порядок пребывания посетителей на объекте. Организация контроля исполнения режимных требований в период пребывания посетителей. Особенности защитных мероприятий, осуществляемых при приеме различных категорий посетителей.	12	Проанализировать материал из источника и учебников: Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М,

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/612572 Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.139-153. Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М. : Проспект : ТК Велби, 2008. - 333 с. – С.193-201. Мосягина Е. Конфиденциальность и защита информации при работе с зарубежными партнерами / Е. Мосягина, Г. Шевцова ; под ред. В. И. Ярочкина. - М. : Паруса, 1999. - 99 с. - С.6-99.
Подготовка к лекции Тема 10. Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности	Понятия «издательская, рекламная и выставочная деятельность», виды, формы, особенности. Обеспечение прав личности на интеллектуальную собственность, при реализации мер по защите информации. Основания к принятию решений по результатам рассмотрения и оценки материалов.	12	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон от 13.03.2006 N 38-ФЗ «О рекламе», Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_58968/. Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.127-139. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов,

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			обучающихся по специальностям: 075200 - Компьютерная безопасность, 075500 - Комплексное обеспечение информ. безопасности автоматизированных систем, 075600 - Информ. безопасность телекоммуникационных систем / [С. Я. Казанцев и др.] ; под ред. С. Я. Казанцева. - М. : Академия, 2005. - 238 с. - (Высшее профессиональное образование. Информационная безопасность) – С.99-145. Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.93-116. Правовое обеспечение информационной безопасности : учебник / [авт.-ред. В. А. Минаев и др.]. - Изд. 2-е, расшир. и доп. - М. : Маросейка, 2008. - 368 с. - (Серия "Информатика и информационная безопасность") – С.195-223. Городов О. А. Информационное право : учебник / О. А. Городов. - М. : Проспект : ТК Велби, 2009. - 242 с. - С.157-199. Сергеев А. П. Право интеллектуальной собственности в Российской Федерации : учебник для студентов вузов, обучающихся по специальности 021100 "Юриспруденция" / А. П. Сергеев. - Изд. 2-е, перераб. и доп. - М. : Проспект, 2004. - 750 с.
Подготовка к лекции Тема 11. Организационная защита конфиденциальных изделий (продукции) в процессе изготовления, хранения, транспортировки и утилизации	Разработка и проведение мероприятий по обеспечению режима конфиденциальности изделий (продукции). Основные требования при хранении, получении, транспортировке и уничтожении изделий.	12	Проанализировать материал из учебников: Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.116-126. Правовое обеспечение информационной безопасности : учебник / [авт.-ред. В. А. Минаев и др.]. - Изд. 2-е, расшир. и доп. - М. :

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
			Маросейка, 2008. - 368 с. - (Серия "Информатика и информационная безопасность") – С.195-223. Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М.: Проспект : ТК Велби, 2008. - 333 с. – С.29-50.
Подготовка к практическому занятию Тема 12. Организация внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности	Цели и задачи внутреннего (служебного) расследования. Процедура внутреннего (служебного) расследования.	12	Проанализировать материал из учебников: Романов О. А. Организационное обеспечение информационной безопасности : учебник для студентов вузов, обучающихся по специальностям "Орг. и технология защиты информ." и "Комплекс. защита объектов информ." направления подгот. "Информ. безопасность" / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 188 с. - (Высшее профессиональное образование. Информационная безопасность) – С.167-173. Организационно-правовое обеспечение информационной безопасности : [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность) – С.116-126. Правовое обеспечение информационной безопасности : учебник / [авт.-ред. В. А. Минаев и др.]. - Изд. 2-е, расшир. и доп. - М. : Маросейка, 2008. - 368 с. - (Серия "Информатика и информационная безопасность") – С.223-276. Городов О. А. Информационное право : учебник / О. А. Городов. - М. : Проспект : ТК Велби, 2009. - 242 с. - С.288-302. Корнеев И. К. Защита информации в офисе : учебник / И. К. Корнеев, Е. А. Степанов ; Гос. ун-т упр. - М.: Проспект : ТК Велби, 2008. - 333 с. – С.76-117.
Подготовка к тестированию	Тема 4. Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. работа с персоналом, имеющим допуск	12	См. ссылки на лекции и практические занятия, материалы которых могут быть полезными при подготовке к промежуточной аттестации, а также рекомендуемые источники и литературу по дисциплине.

Вид работы	Содержание (перечень вопросов)	СРС (в час.)	Рекомендации
	(доступ).		
Подготовка к контрольной работе	Тема 2. Сущность организационного обеспечения информационной безопасности Тема 3. Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности Тема 5. Организация системы доступа к защищаемой информации (сведениям, документам, изделиям) Тема 6. Организация пропускного и внутри объектового режимов Тема 7. Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями	12	См. ссылки на лекции и практические занятия, материалы которых могут быть полезными при подготовке к промежуточной аттестации, а также рекомендуемые источники и литературу по дисциплине.
Подготовка к промежуточной аттестации (экзамен)	Темы дисциплины	12	См. ссылки на лекции и практические занятия, материалы которых могут быть полезными при подготовке к промежуточной аттестации, а также рекомендуемые источники и литературу по дисциплине.
Итого по дисциплине		128	

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Организационное обеспечение информационной безопасности» реализует в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация (степень) «бакалавр»), утвержденного и введенного в действие приказом Министерства образования и науки РФ от 01 декабря 2016 г. № 1515.

Дисциплина «Организационное обеспечение информационной безопасности» входит в базовую часть цикла дисциплин подготовки студентов по направлению подготовки 10.03.01 «Информационная безопасность».

Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности Института информационных наук и технологий безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с теоретическими и практическими проблемами формирования и функционирования систем организационного и правового обеспечения информационной безопасности, а также формированием практических навыков по организационной защите информации и применению норм права в области информационной безопасности.

Цель курса: формирование знаний по теоретическим и практическим проблемам функционирования систем организационного и правового обеспечения информационной безопасности с целью формирования практических навыков по организационной защите информации и применению норм права в области информационной безопасности. Способствовать в подготовке специалиста, умеющего сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельность, основу которой составляет организационная работа.

Задачи курса:

- изучить базовые теоретические понятия, лежащие в основе мероприятий по организационному и правовому обеспечению информационной безопасности;

- овладеть практическими организационными методами защиты информации на объектах информатизации;

- овладеть необходимой юридической терминологией;

- сформировать взгляды на обеспечение информационной безопасности как на

системную научно-практическую деятельность, основу которой составляет организационная работа.

Дисциплина направлена на формирование следующих компетенций:

- УК-2 - Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

В результате освоения дисциплины обучающийся должен:

- Уметь анализировать имеющиеся ресурсы и ограничения, оценивать и выбирать оптимальные способы решения поставленных задач
- Уметь использовать знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.

- ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

В результате освоения дисциплины обучающийся должен:

- Уметь применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
- Уметь обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав
- Владеть навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации

- ОПК-6 - Способен при решении профессиональных задач организовывать защиту 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;

В результате освоения дисциплины обучающийся должен:

- Знать нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите

информации

- Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации
- Владеет навыками по разработке политики безопасности объекта информатизации

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестирования, контрольной работы, промежуточная аттестация в форме экзамена

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы.