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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Рабочая программа дисциплины

Составитель:
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры
Информационной безопасности
№ 9 от 17.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины (модуля): формирование культуры информационной безопасности (ИБ) в социальной среде.

Задачи дисциплины:

- изучение основных угроз ИБ в социальной среде;
- формирование знаний у обучающихся о правовых и организационных принципах обеспечения ИБ в социальной среде;
- выработка у обучающихся практических умений по использованию методов обеспечения ИБ.

Цель курса: сформировать взгляд на правовое обеспечение информационной безопасности как на системную научно-практическую деятельность, одну из основ которой составляет работа по нормативно-правовому обеспечению информационной безопасности.

Задачи курса:

- изучить конституционные гарантии прав граждан на доступ к информации, в том числе права свободно искать, получать, передавать, производить и распространять информацию любым законным способом с учетом особенностей реализации этих прав в отношении информации ограниченного доступа;
- освоить основы правового регулирования отношений в информационной сфере, меры и средства организационно-правового обеспечения информационной безопасности и защиты информации ограниченного доступа, в том числе основополагающие государственные стандарты РФ в области информационной безопасности и защиты информации;
- рассмотреть понятие тайны как правового режима ограничения доступа к информации, в том числе правового режима государственной тайны и иных видов тайн, особенности правового регулирования отношений в сфере обращения информации о персональных данных граждан;
- изучить правовые основы и порядок сертификации средств защиты информации и практику правового регулирования лицензионной деятельности в области информационной безопасности и защиты информации ограниченного доступа.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

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, имеющихся ресурсов и ограничений	УК-2.1 Уметь анализировать имеющиеся ресурсы и ограничения, оценивать и выбирать оптимальные способы решения поставленных задач	Знать особенности государственно-конституционного устройства и правовые основ современного Российского государства, соотношения прав отдельных личностей, общества и государства в целом, а также характеристики и содержание основных отраслей права;
	УК-2.2 Уметь использовать знаний о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения.	Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать основы правовых знаний в

		различных сферах деятельности
УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Знает сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями	Знать: закономерности развития предприятий различного типа и организацию их функционирования с целью достижения максимальной эффективности при минимальных затратах ресурсов.
	УК-10.2 Умеет анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению	Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
	УК-10.3 Владеет навыками работы с законодательными и другими нормативными правовыми актами	Владеть: навыками использовать основы правовых 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	Знать особенности государственно-конституционного устройства и правовые основ современного Российского государства, соотношения прав отдельных личностей, общества и государства в целом, а также характеристики и содержание основных отраслей права;
	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	Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
	ОПК-5.3 Владеть навыками разрабатывать проекты локальных правовых документов, регламентирующих работу по обеспечению информационной безопасности в организации	Владеть: навыками использовать основы правовых знаний в различных сферах деятельности
ОПК-6 - Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими	ОПК-6.1 Знать нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знать особенности государственно-конституционного устройства и правовые основ современного Российского государства, соотношения прав отдельных личностей, общества и государства в целом, а также характеристики и содержание основных отраслей права;

документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.2 Умеет разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации	Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
	ОПК-6.3 Владеет навыками по разработке политики безопасности объекта информатизации	Владеть: навыками использовать основы правовых знаний в различных сферах деятельности

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Правовое обеспечение информационной безопасности» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Основы информационной безопасности», «Специальное документоведение и документационное обеспечение управления».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для прохождения дисциплин Технологическая практика, Эксплуатационная практика, Преддипломная практика.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 6 з.е., 216 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	**22**
3	Практические занятия	**24**
4	Лекции	**26**
4	Практические занятия	**32**
	Всего:	**104**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 112 академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
	Тема 1. Введение. Информационная безопасность как определяющий компонент	Предмет и содержание дисциплины, методы ее изучения, источники и литература, контроль освоения.

	национальной безопасности России.	Направления государственной политики РФ по обеспечению информационной безопасности личности, общества и государства. Доктрина информационной безопасности РФ. Понятия «правовое обеспечение информационной безопасности» и «правовая защита информации». Определение указанных понятий по целям, функциям, структуре.
	Тема 2. Право на информацию. Право на доступ к информации.	Составляющие права на информацию. Законодательство о праве на информацию. Право на доступ к информации, в том числе к информации о деятельности органов государственной власти и местного самоуправления.
	Тема 3. Информационная сфера как объект правовых отношений.	Понятие информационной сферы и ее составляющие. Информация как объект гражданско-правовых отношений. Правовые принципы защиты информации. Информационные системы как объекты правовых отношений. Место правовой защиты информации в системе комплексной защиты информации.
	Тема 4. Закон РФ «Об информации, информационных технологиях и защите информации» как организационно-правовая основа регулирования правоотношений в информационной сфере.	Сфера действия Закона. Основные понятия, используемые в Законе. Права обладателя информации. Порядок распространения или предоставления информации. Порядок документирования информации. Государственное регулирование в сфере применения информационных технологий. Порядок обеспечения защиты информации.
	Тема 5. Правовое обеспечение защиты документированной информации с ограниченным доступом. Стандарты информационной безопасности.	Принципы правового обеспечения защиты документированной информации с ограниченным доступом. Меры и средства организационно-правовой защиты информации ограниченного доступа как необходимое условие обеспечения информационной безопасности для организации любой формы собственности. Основополагающие государственные стандарты РФ в области информационной безопасности и защиты информации Документационное обеспечение защиты информации в организации любой формы собственности.
	Тема 6. Тайна как правовой режим ограничения доступа к информации.	Разновидности правового режима информации. Правовой режим ограниченного доступа к информации**.** Виды информации ограниченного доступа. Виды конфиденциальной информации. Понятие государственной тайны, основные

		положения законодательства о государственной тайне. Правовое регулирование режимов коммерческой тайны, служебной тайны, банковской тайны и профессиональных тайн. Право на секрет производства (ноу-хау). Служебный секрет производства
	Тема 7. Правовое регулирование отношений в сфере обращения информации о персональных данных граждан.	Основные понятия законодательства о персональных данных, разница между понятиями «неприкосновенность частной жизни» и «персональные данные» как объектов права. Общедоступные источники персональных данных. Специальные категории персональных данных. Биометрические персональные данные. Принципы и условия обработки персональных данных. Права субъекта персональных данных. Обязанности оператора при обработке персональных данных. Права уполномоченного органа по защите прав субъектов персональных данных. Классификация информационных систем персональных данных. Основные методы и способы защиты информации в информационных системах персональных данных для различных классов этих систем.
	Тема 8. Правовые особенности сертификации средств защиты информации и правовое регулирование лицензионной деятельности в области защиты информации.	Понятие сертификации и общие положения о сертификации средств защиты информации. Технические регламенты и стандарты. Подтверждение соответствия. Информация о нарушении требований технических регламентов и стандартов. Порядок лицензирования деятельности по технической защите конфиденциальной информации и по разработке и/или производству средств защиты конфиденциальной информации.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1	Введение. Информационная безопасность как определяющий компонент национальной безопасности России	Лекция 1	Вводная лекция с использованием презентационного материала
2	Право на информацию. Право на	Лекция 2 Практические	Лекция-дискуссия с использованием презентационного

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
	доступ к информации	занятия 1-2	материала
3	Информационная сфера как объект правовых отношений	Лекция 3 Практическое занятие 3	Лекция-дискуссия с использованием презентационного материала, контрольная работа
4	Закон РФ «Об информации, информационных технологиях и защите информации» как организационно-правовая основа регулирования правоотношений в информационной сфере	Лекция 4 Практические занятия 4	Лекция-дискуссия с использованием презентационного материала, контрольная работа
5	Правовое обеспечение защиты документированной информации с ограниченным доступом. Стандарты информационной безопасности	Лекция 5 Практические занятия 5-6	Лекция-дискуссия с использованием презентационного материала Тестирование
6	Тайна как правовой режим ограничения доступа к информации – государственная тайна, служебная тайна, коммерческая тайна, профессиональные тайны	Лекции 6-11 Практические занятия 7-14	Лекция с использованием презентационного материала Тестирование
7	Правовое регулирование отношений в сфере обращения информации о персональных данных граждан	Лекция 12 Практические занятия 15-16	Лекция-дискуссия Консультирование и проверка домашних заданий посредством электронных носителей
8	Правовые особенности сертификации средств защиты информации и правовое регулирование лицензионной деятельности в области защиты информации	Практические занятия 17-18	Консультирование и проверка домашних заданий посредством электронных носителей

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Максимальное количество баллов	
	За одну работу	Всего
Текущий контроль: - тестирование - контрольная работа - практическая работа	 4 балла 10 баллов 12 баллов	 28 баллов 20 баллов 12 баллов
Промежуточная аттестация - зачет с оценкой, экзамен (ответы на вопросы)	40 баллов	
Итого за семестр	100 баллов	

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	отлично/ 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	хорошо/ 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 –

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		«хороший».
67-50/ D,E	удовлетво-рительно/ 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	неудовлет-ворительно/ 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

Текущий контроль (примерное ситуационное задание для практической работы по теме 5, 8) - проверка сформированности компетенций - УК-2; УК-10; ОПК-5; ОПК-6

В качестве специалиста в области организации и технологии защиты информации Вы вступили в должность начальника отдела защиты информации (службы безопасности) в ранее созданной и успешно работающей в настоящее время организации. Эта организация подведомственна _____.
Основным видом деятельности этой организации в течение ряда лет являлась разработка _____

На эту организацию в ближайшие три-четыре месяца будет возложена дополнительная обязанность по разработке и серийному производству средств защиты _____.

Перечислите и обоснуйте последовательность Ваших организационно-правовых действий, необходимых для успешного выполнения поставленной задачи, в том числе:
- необходимость получения лицензии на указанный вид новой деятельности и наименование организации, в которую Вы будете обращаться для получения лицензии;
- порядок Вашего взаимодействия с этой организацией и перечень документов, которые должны быть представлены Вами в эту организацию;

- основные лицензионные требования и условия, которые должны быть выполнены Вами для получения лицензии и срок действия получаемой лицензии;
- необходимость создания нового подразделения в рамках отдела по защите информации;
- необходимость организации сертификации производимых Вами средств защиты информации, система сертификации, в которую Вы должны будете обратиться и схема проведения сертификации этих средств.

Текущий контроль (примерный тест по теме 6) – проверка сформированности компетенций - УК-2; УК-10; ОПК-5; ОПК-6

Укажите номер правильного ответа

1.. Доступ к сведениям, составляющим государственную тайну это?

1.1. Санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

1.2. Процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.

1.3. Процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну.

1.4. Санкционированное ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Укажите номер правильного ответа

2. На основании чего устанавливается порядок доступа должностного лица или гражданина к сведениям, составляющим государственную тайну?

2.1. На основании нормативных документов, утвержденных Правительством Российской Федерации.

2.2. На основании нормативных документов, утвержденных Федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

2.3. На основании нормативных документов, утвержденных руководителем предприятия.

2.4. На основании нормативных документов, утвержденных руководителем подразделения по защите государственной тайны.

Укажите номер правильного ответа

3. Кто осуществляет законодательное регулирование отношений в области государственной тайны?

3.1. Органы судебной власти.

3.2. Правительство Российской Федерации.

3.3. Палаты Федерального Собрания.

3.4. Органы государственной власти Российской Федерации.

Укажите номер правильного ответа

4. Информацию в зависимости от порядка ее предоставления или распространения подразделяют?

4.1.На свободно распространяемую.

4.2. На распространяемую между Федеральными органами исполнительной власти.

4.3. На распространяемую только в особых случаях.

4.4. На информацию перечисленную во всех вышеперечисленных пунктах.

Укажите номер правильного ответа

5. Кто вносит в полномочные органы государственной власти предложения по

совершенствованию системы защиты государственной тайны?

5.1. Президент Российской Федерации.

5.2. Правительство Российской Федерации.

5.3. Палаты Федерального Собрания.

5.4. Органы государственной власти Российской Федерации.

Укажите номер правильного ответа

6. Обладатель информации, составляющей коммерческую тайну, имеет право?

6.1. Защищать в установленном законом порядке свои права в случае незаконного использования третьими лицами информации, составляющей коммерческую тайну.

6.2. Запрещать доступ к информации, составляющей коммерческую тайну.

6.3. Требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации.

6.4. Использовать все права указанные выше.

Укажите номер правильного ответа

7. Исключительное право на результат интеллектуальной деятельности это?

7.1. Охраняемая правом возможность правообладателя по своему усмотрению любым не противоречащим закону способом использовать объект интеллектуальной собственности, результат интеллектуальной деятельности или средство индивидуализации, распоряжаться им, разрешать или запрещать другим лицам его использование.

7.2. Охраняемая правом возможность правообладателя по своему усмотрению использовать объект интеллектуальной собственности, результат интеллектуальной деятельности или средство индивидуализации, распоряжаться им, разрешать или запрещать другим лицам его использование.

7.3. Охраняемая правом возможность использовать объект интеллектуальной собственности, результат интеллектуальной деятельности или средство индивидуализации, распоряжаться им, разрешать или запрещать его использование.

7.4. Охраняемая правом возможность правообладателя по своему усмотрению использовать объект интеллектуальной собственности, результат интеллектуальной деятельности, распоряжаться им, разрешать или запрещать другим лицам его использование.

Укажите номер правильного ответа

8. Информационные технологии, представляющие собой процессы и (или) методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов являются?

8.1. Субъектом правового режима.

8.2. Объектом правового режима.

8.3. Техническими средствами информационных систем.

8.4. Всеми перечисленными определениями.

Укажите номер правильного ответа

9. Право на средства индивидуализации предприятий вкючает?

9.1. Право на коммерческое обозначение.

9.2. Право на оборот товара независимо от его места происхождения.

9.3. Право на знак качества.

9. 4. Все вышеперечисленные права.

Укажите номер правильного ответа

10. Правоприменительная деятельность это?

10.1. Установление определенных правовых норм осуществления наиболее важных общественных отношений и охраны этих норм от нарушения с использованием государственного принуждения.

10.2. Подготовка, принятие и издание законодательными органами нормативных правовых актов, регулирующих отношения в области удовлетворения национальных интересов в информационной сфере, а также создающих условия для предотвращения реализации угроз информационной безопасности.

10.3. Реализация функции государства по обеспечению правосудия в процессе выполнения задач противодействия угрозам информационной безопасности.

10.4. Основанная на законодательстве оперативная, повседневная реализация органами исполнительной власти (государственного управления) функций государства в области обеспечения информационной безопасности.

Примерные контрольные вопросы к промежуточной аттестации по курсу – проверка сформированности компетенций **- УК-2; УК-10; ОПК-5; ОПК-6**

1. Понятие «национальная безопасность». Информационная безопасность как составная часть национальной безопасности.
2. Понятие «информационная сфера», ее структура. Объекты отношений в информационной сфере. Понятие «информация». Понятия «сведения» и «сообщения» в информационных отношениях. Особенности информации как объекта права. Правовые принципы защиты информации.
3. Сфера действия Закона РФ «Об информации, информационных технологиях и защите информации» и основные понятия, используемые в этом Законе.
4. Правовое обеспечение защиты документированной информации с ограниченным доступом, меры и средства, используемые для организации защиты такой информации.
5. Документационное обеспечение защиты документированной информации ограниченного доступа в организации любой формы собственности.
6. Понятие «информационная система» в Законе РФ «Об информации, информационных технологиях и защите информации». Информационная система (ИС) как объект защиты информации.
7. Основные принципы разработки и реализации политики информационной безопасности в информационной системе. Основополагающие стандарты в области информационной безопасности и защите информации.
8. Классификация информации по режиму доступа к ней. Понятие правового режима обращения информации. Правовые режимы свободного доступа к информации.
9. Правовой режим ограниченного доступа к информации, реализуемый на основе понятия «тайна». Тайна как правовая категория и её соотношение с понятием информация. Общий признак всех видов тайн.
10. Определение понятия «государственная тайна». Сфера действия федерального закона «О государственной тайне». Объект и субъекты правоотношений в области государственной тайны.
11. Принципы отнесения сведений к государственной тайне и их засекречивания. Основной критерий выбора степени секретности. Сведения, не подлежащие засекречиванию. Система перечней сведений, составляющих государственную тайну, их роль в системе засекречивания.
12. Иерархия органов защиты государственной тайны и их основные функции. Основные права государства в отношении сведений, относящихся к государственной тайне.

13. Порядок допуска должностных лиц и граждан к сведениям, составляющим государственную тайну, Основания для отказа в получении допуска. Формы допуска в соответствии со степенями секретности. Правовые последствия оформления допуска. Субъекты особого порядка допуска.
14. Развитие российского законодательства о служебной тайне. Признаки, необходимые для отнесения информации к служебной тайне. Основные объекты служебной тайны. Перечень сведений, которые не могут быть отнесены к служебной тайне. .
15. Порядок правовой охраны конфиденциальной информации, переданной в государственный орган исполнительной власти юридическими или физическими лицами – субъектами предпринимательской или иной деятельности. Приведите примеры.
16. Права руководителя федерального государственного органа исполнительной власти в качестве обладателя в отношении собственной служебной тайны и способ реализации этих прав.
17. Основные понятия федерального закона «О коммерческой тайне». Информация, которая может быть отнесена к коммерческой тайне. Законодательно установленный перечень информации, которая не может быть отнесена к коммерческой тайне.
18. Обязательные и факультативные составляющие, используемые для установления режима коммерческой тайны субъектами предпринимательской деятельности. Обязанности работника и работодателя в сфере коммерческой тайны. Виды ответственности за правонарушения в сфере коммерческой тайны.
19. Понятие «профессиональная тайна» и признаки, необходимые для отнесения информации к профессиональной тайне. Субъекты правоотношений для основных видов профессиональных тайн, приведите примеры.
20. Банковская тайна как вид профессиональной тайны и законодательное определение этого понятия. Место банковской тайны в числе иных видов тайн в массиве конфиденциальной информации, которая накапливается, хранится и используется в банковской деятельности.
21. Определение понятий «банковская тайна» и «коммерческая тайна банка», принципиальные различия между этими понятиями. Основные права обладателя банковской тайны (клиента банка) в отношении информации, составляющей его банковскую тайну.
22. Обязанности банка по сохранению и защите конфиденциальной информации обладателей банковской тайны – клиентов банка, которая была получена банком в качестве пользователя этой информацией на законных основаниях. Возможные случаи ограничения прав клиентов банка на защиту такой информации.
23. Основные понятия, используемые в федеральном законе «О персональных данных». Разница между понятиями «неприкосновенность частной жизни» и «персональные данные» как объектов права.
24. Понятие конфиденциальности персональных данных. Общедоступные источники персональных данных. Специальные категории персональных данных. Биометрические персональные данные.
25. Право субъекта персональных данных на доступ к своим персональным данным. Обязанности оператора по обеспечению безопасности персональных данных при их обработке. Порядок уведомления оператором уполномоченного органа по защите прав субъектов персональных данных.
26. Понятие информационной системы персональных данных. Классификация информационных систем персональных данных.
27. Общие положения законодательства о лицензировании определенных видов деятельности, достоинства и недостатки любой системы лицензирования. Лицензирование деятельности в защиты информации как правовая форма обеспечения информационной безопасности.
28. Правовые особенности лицензирования деятельности по технической защите конфиденциальной информации и по разработке и (или) производству средств защиты конфиденциальной информации.
29. Правовые основы лицензирования деятельности организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну.

30. Основные понятия ФЗ РФ «О техническом регулировании» (сертификация, стандарт, технический регламент, форма подтверждения соответствия). Организация государственной сертификации средств защиты информации (ЗИ). Органы исполнительной власти, создающие системы сертификации средств ЗИ, участники любой системы сертификации средств ЗИ. Испытательные лаборатории их права и обязанности

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Конституция Российской Федерации (принята всенародным голосованием 12.12.1993), Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/

Гражданский кодекс Российской Федерации. Часть первая, от 30.11.1994 N 51-ФЗ Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/

Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ, Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/

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/

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/

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/

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/

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/

Федеральный закон от 09.02.2009 N 8-ФЗ "Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_84602/

Федеральный закон от 31.05.2002 N 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_36945/

Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации" Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7054/

ГОСТ Р ИСО/МЭК 17799-2005 "Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст), Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=447600#013921417480764586

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст), Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=EXP;n=418509# 08480021357350149

Литература

Основная

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

Дополнительная

Организационно-правовое обеспечение информационной безопасности: [учеб. пособие] / [А. А. Стрельцов и др.] ; под ред. А. А. Стрельцова. – М.: Академия, 2008. – 248с. 10 э.

Государственная тайна и ее защита в Российской Федерации: учеб. пособие для студентов вузов / П. П. Аникин [и др.]; под общ. ред.: М. А. Вуса и А. В. Федорова. – 3-е изд., испр. и доп. – СПб.: Юрид. центр Пресс, 2007. – 745с.

Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (Обложка. КБС) ISBN 978-5-00091-007-8 - Режим доступа: http://znanium.com/catalog/product/544554

Правовое обеспечение информационной безопасности: Учебник / [авт.-ред. В. А. Минаев и др.]. – Изд. 2-е, расширенное и доп. – М.: Маросейка, 2008. – С. 120-124.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:

1. Консультант Плюс

2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

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

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox

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. Право на доступ к информации

Вопросы для изучения и обсуждения:

1. Теоретические основы и границы права на информацию.
2. Законодательство о праве на информацию. Субъекты права на информацию.
3. Содержание права граждан на информацию.
4. Право на доступ к информации о деятельности органов государственной власти и местного самоуправления.

Контрольные вопросы:

1. Назовите основные принципы обеспечения права на доступ к информации.
2. Приведите основные формы реализации конституционного права граждан на доступ к информации.
3. Перечислите законодательно установленные способы обеспечения доступа к информации о деятельности государственных и органов местного самоуправления.
4. Перечислите основное содержание информации о деятельности государственных и органов местного самоуправления в Интернете.

Практические занятия 2, тема 4. Закон РФ «Об информации, информационных технологиях и защите информации» как организационно-правовая основа регулирования правоотношений в информационной сфере

Вопросы для изучения и обсуждения:

1. Основные понятия, используемые в законе.
2. Принципы разделения информации на категории открытого и ограниченного доступа.
3. Порядок распространения информации или предоставления информации.
4. Порядок документирования информации.
5. Информационная система как объект правового регулирования.
6. Государственное регулирование в сфере применения информационных технологий. Государственные информационные системы.
7. Регулирование отношений в сфере защиты информации

Контрольные вопросы:

1. Раскройте на примерах содержание основных понятий, используемых в Законе – информация, конфиденциальность информации, предоставление и распространения информации.
2. Перечислите виды информации, относимой к категории ограниченного доступа, дайте им краткую характеристику.
3. Определите возможный порядок документирования и перечислите формы представления документированной информации.
4. Какие требования предусматривает государственный порядок распространения информации.
5. Перечислите основные признаки информационной системы как объекта правового регулирования.
6. Перечислите обязанности обладателя и пользователя информации, а также оператора информационной системы по защите информации ограниченного доступа.

Практическое занятие 3, тема 5. Правовое обеспечение защиты информации с ограниченным доступом. Стандарты информационной безопасности

Вопросы для изучения и обсуждения:

1. Разновидности правовых режимов информации.
2. Основные законодательно определенные виды информации ограниченного доступа.
3. Меры и средства, используемые для защиты информации с ограниченным доступом.
4. Основные положения Закона РФ «О техническом регулировании» в части стандартизации.
5. Основные положения действующих стандартов РФ в области информационной безопасности и защиты информации.

Контрольные вопросы:

1. Перечислите основные законодательно определенные виды информации ограниченного доступа и дайте им краткую характеристику.
2. Перечислите меры и средства, используемые в рамках известных видов защиты информации (правовой, организационной, инженерно-технической и программно-аппаратной) с целью обеспечения информационной безопасности организации любой формы собственности.
3. Понятие стандартизация, цели стандартизации и виды стандартов.
4. Основные положения стандарта ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт России.
5. Основные положения стандарта ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью.
6. Основные положения стандарта ГОСТ Р ИСО/МЭК 27001-2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

Практическое занятие 4, тема 6. Тайна как правовой режим ограничения доступа к информации – государственная тайна (далее ГТ)

Вопросы для изучения и обсуждения:

1. Сфера действия ФЗ РФ «О государственной тайне» (далее Закон) и основные понятия Закона.

2. Понятие о перечнях сведений, составляющих ГТ и степени секретности сведений.

3. Порядок отнесения сведений к ГТ и принципы их засекречивания. Сведения, не подлежащие засекречиванию.

4. Порядок рассекречивания сведений и их носителей.

5. Распоряжение сведениями, составляющими ГТ.

6. Иерархия органов защиты ГТ.

7. Порядок допуска должностных лиц и граждан к ГТ, основания для отказа в допуске и условия прекращения допуска.

8. Лицензирование деятельности, связанной с использованием ГТ, как обязательное условие допуска предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих ГТ.

9. Ответственность за нарушение законодательства РФ о ГТ.

Контрольные вопросы:

1. Определение понятия «государственная тайна» (ГТ). Сфера действия закона РФ «О ГТ». Объект правоотношений на ГТ. Субъекты правоотношений в области ГТ. Принципы отнесения сведений к государственной тайне (ГТ) и засекречивания этих сведений.

2. Понятие о перечнях сведений, составляющих государственную тайну (ГТ). Основной критерий выбора степени секретности. Порядок рассекречивания сведений, относящихся к государственной тайне. Понятие о комиссионном порядке рассекречивания.

3. Иерархия органов защиты государственной тайны и их основные функции. Порядок допуска организаций к проведению работ, связанных с использованием информации, составляющей государственную тайну.

4. Основные права государства в отношении сведений, относящихся к категории государственной тайны.

5. Порядок допуска должностных лиц и граждан к сведениям, составляющим государственную тайну. Основания для отказа в получении допуска. Формы допусков в соответствии с грифами сведений.

6. Разница между понятиями «допуск» и «доступ» должностного лица или гражданина к сведениям, составляющим государственную тайну. Конкретный порядок организации доступа работника к секретным документам.

7. Ответственность за нарушение законодательства о государственной тайне.

Практическое занятие 5, тема 7 (2 часа). Правовое регулирование отношений в сфере обращения информации о персональных данных граждан (далее ПДн)

Вопросы для изучения и обсуждения:

1. Общие положения и основные понятия, используемые в Законе РФ «О персональных данных».

2. Принципы и условия обработки ПДн.

3. Классификация ПДн – общедоступные, специальные, биометрические.

4. Основные права субъекта ПДн.

5. Основные обязанности оператора ПДн.

6. Государственный контроль и надзор за обработкой ПДн, ответственность за нарушение требований законодательства о ПДн.

7. Понятие информационной системы обработки ПДн.

Контрольные вопросы:

1. Определите разницу между понятиями «неприкосновенность частной жизни» и «персональные данные» как объектов права.

2. Конфиденциальность ПДн как основной принцип их обработки.

3. Определите разницу между понятиями «обработка ПДн» и «оборот ПДн».

4. Перечислите права субъекта на получение информации, касающейся обработки его ПДн и возможные случаи ограничения этих прав.

5. Перечислите меры по обеспечению безопасности ПДн, принимаемые оператором ПДн при их обработке.

6. Порядок уведомления оператором органа по защите прав субъектов ПДн о намерении их обработки, и случаи законодательно установленного права оператора на обработку ПДн без такого уведомления.

7. Принципы классификации информационных систем обработки ПДн.

Практическое занятие 6, тема 8 (2 часа). Правовое регулирование лицензионной деятельности в области защиты информации

Вопросы для изучения и обсуждения:

1. Лицензирование предпринимательской деятельности: достоинства и недостатки

1. Сфера применения закона РФ «О лицензировании отдельных видов деятельности» и основные понятия этого Закона.

2. Общие правовые принципы осуществления лицензионной деятельности.

3. Лицензирования деятельности в области защиты информации как необходимое условие обеспечения информационной безопасности.

4. Ответственность за нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации.

Контрольные вопросы:

1. Перечислите органы исполнительной власти, уполномоченные лицензировать деятельность в области технической защиты, а также в области разработки и производства средств защиты конфиденциальной информации.

2. Перечислите виды работ и услуг по технической защите конфиденциальной информации, осуществляемых юридическими лицами и индивидуальными предпринимателями и подлежащих лицензированию.

3. Перечислите виды работ, выполняемых юридическими лицами и индивидуальными предпринимателями при разработке и (или) производству средств защиты конфиденциальной информации и подлежащих лицензированию.

Практическое занятие 7. Организация работы по определению состава, засекречиванию и рассекречиванию (введению и снятию ограничения доступа) информации (2 часа)

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.

Практическое занятие 8. Лицензирование деятельности предприятий в области организационного обеспечения информационной безопасности (4 часа) -

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?

Практическое занятие 9. Определение должностей и подбор персонала для работы с конфиденциальной информацией. Оформление допуска граждан к государственной тайне. Работа с персоналом, имеющим допуск (доступ) (4 часа)

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.

Практическое занятие 10. Организация системы доступа к защищаемой информации (сведениям, документам, изделиям) (2 часа)

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.

Практическое занятие 11. Организация пропускного и внутри объектового режимов (4 часа)

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?

Практическое занятие 12. Организационные требования к помещениям, в которых ведутся работы с конфиденциальными документами и изделиями (2 часа)

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.

Практическое занятие 13. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам (2 часа)

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.

Практическое занятие 14. Организация защиты информации при приеме на объекте посетителей (2 часа)

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?

Практическое занятие 15. Организация защиты информации при осуществлении издательской, рекламной и выставочной деятельности (4 часа)

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?

Практическое занятие 16. Организационная защита конфиденциальных изделий (продукции) в процессе изготовления, хранения, транспортировки и утилизации (2 часа)

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?

Практическое занятие 17. Организация внутреннего (служебного) расследования по фактам нарушения режима конфиденциальности (4 часа

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?

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

Цель курса: сформировать взгляд на правовое и организационное обеспечение информационной безопасности как на системную научно-практическую деятельность, одну из основ которой составляет работа по нормативно-правовому обеспечению информационной безопасности, формированию и функционированию систем организационного и правового обеспечения информационной безопасности.

Задачи курса:

- изучить конституционные гарантии прав граждан на доступ к информации, в том числе права свободно искать, получать, передавать, производить и распространять информацию любым законным способом с учетом особенностей реализации этих прав в отношении информации ограниченного доступа;
- освоить основы правового регулирования отношений в информационной сфере, меры и средства организационно-правового обеспечения информационной безопасности и защиты информации ограниченного доступа, в том числе основополагающие государственные стандарты РФ в области информационной безопасности и защиты информации;
- рассмотреть понятие тайны как правового режима ограничения доступа к информации, в том числе правового режима государственной тайны и иных видов тайн, особенности правового регулирования отношений в сфере обращения информации о персональных данных граждан;
- изучить правовые основы и порядок сертификации средств защиты информации и практику правового регулирования лицензионной деятельности в области информационной безопасности и защиты информации ограниченного доступа.
- сформировать взгляды на обеспечение информационной безопасности как на системную научно-практическую деятельность, основу которой составляет организационная работа.
- разрабатывать проекты локальных нормативных документов, регламентирующих защиту информации ограниченного доступа в организации
- разрабатывать политику безопасности объекта информатизации

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.

УК-10 - Способен формировать нетерпимое отношение к коррупционному поведению

В результате освоения дисциплины обучающийся должен:

- Знает сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями
- Умеет анализировать, толковать и правильно применять правовые нормы о противодействии коррупционному поведению

- Владеет навыками работы с законодательными и другими нормативными правовыми актами

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

По дисциплине предусмотрена промежуточная аттестация в форме зачёта с оценкой (3 семестр), экзамена (4 семестр).

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц.