Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.04.01 Информационная безопасность

Наименование образовательной программы: Управление информационной безопасностью

Уровень образования: высшее образование - магистратура

Форма обучения: Очная

Оценочные материалы
по дисциплине
Организационно-правовые механизмы обеспечения информационной безопасности

Москва
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Трофимцева С.Ю. Идентификатор: Rdda85afd-TrofimtsevaSY-5aba752	С.Ю. Трофимцева

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-3 Способен разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности

ИД-1 Организует работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России

и включает:

для текущего контроля успеваемости:

Форма реализации: Компьютерное задание

1. Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности (Тестирование)
2. Киберпреступления. Основные механизмы противодействия киберпреступности (Тестирование)
3. Классификация информации по доступу и видам тайн (Тестирование)
4. Правовой статус информации. правовое регулирование информационных отношений (Тестирование)

БРС дисциплины

2 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности					
Введение в дисциплину		+			
Теоретико-правовой базис регулирования отношений в сфере информационной безопасности		+			
Правовой статус информации. правовое регулирование информационных отношений					
Правовой статус информации			+		+
Правовое регулирование информационных отношений			+		+
Информационная безопасность в системе национальной безопасности					

Национальная безопасность: содержание, виды		+		
Информационная безопасность как вид национальной безопасности и её элементы. Структура федеральных органов власти, обеспечивающих информационную безопасность РФ		+		
Киберпреступления. Основные механизмы противодействия киберпреступности				
Генезис киберпреступности. Современные проблемы эффективного противодействия киберпреступлениям			+	
Уголовно-правовое и уголовно-процессуальное противодействие киберпреступности на международном и национальном уровнях			+	
Классификация информации по доступу и видам тайн				
Виды классификаций информации по доступу и распространению. Информация, свободно распространяемая, негативная информация				+
Защищаемая информация ограниченного доступа, не содержащая тайну				+
Защищаемая информация в режиме тайн				+
Вес КМ:	10	25	30	35

БРС курсовой работы/проекта

2 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Введение		+			
Глава 1			+		
Глава 2				+	
Заключение					+
Вес КМ:		10	40	40	10

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-3	ИД-1$_{ОПК-3}$ Организует работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России	Знать: структуру, задачи и функции органов, регулирующих деятельность объектов и субъектов в сфере ИБ систему нормативного правового регулирования защиты определённого вида информации и прав её обладателя принципы работы с правовыми нормами, относящимися к различным правовым системам и отраслям права, в профессиональных ситуациях в сфере информационной безопасности обстоятельства возникновения уголовной и административной ответственности при	Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности (Тестирование) Правовой статус информации. правовое регулирование информационных отношений (Тестирование) Киберпреступления. Основные механизмы противодействия киберпреступности (Тестирование) Классификация информации по доступу и видам тайн (Тестирование)

		возникновении ИБ-инцидента содержание доктринальных документов РФ в сфере информационной безопасности принципы правового регулирования информационных отношений Уметь: использовать правовые нормы для разрешения конфликтов и инцидентов в сфере информационной безопасности определять необходимые правовые нормы для защиты определённого вида информации и формирования политики безопасности информации и защиты информационных прав субъекта в организации определять вид правонарушения в киберсфере и перечень требуемых мер при его выявлении	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Введение в дисциплину. Теоретико-правовой базис регулирования отношений в сфере информационной безопасности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Учебная группа. Компьютерный класс. СДО «Прометей». Продолжительность: 1 учебный час

Краткое содержание задания:
Ответить на вопросы теста

Контрольные вопросы/задания:

Знать: принципы работы с правовыми нормами, относящимися к различным правовым системам и отраслям права, в профессиональных ситуациях в сфере информационной безопасности	1.Что не относится к признакам права в информационной сфере? 2.Что не относится к нормативным правовым актам в РФ, регулирующим информационную сферу?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если вопросы теста даны полностью или в основном правильные ответы

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если на значительную часть вопросов даны правильны ответы

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если больше чем на половину вопросов даны правильные ответы

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется, если менее чем на половину вопросов даны правильные ответы

КМ-2. Правовой статус информации. правовое регулирование информационных отношений

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Учебная группа. Компьютерный класс. СДО «Прометей». Продолжительность: 1 учебный час

Краткое содержание задания:
Ответить на вопросы теста

Контрольные вопросы/задания:

Знать: принципы правового регулирования информационных отношений	1.Что именно исследователи не относят к целям субъектов информационных отношений?
Знать: содержание доктринальных документов РФ в сфере информационной безопасности	1.К чему, согласно Стратегии национальной безопасности РФ 2021 г., не приводит усиливающаяся нестабильность в мире? 2.В каких официальных документах, излагающих официальные взгляды на проблемы безопасности (национальной безопасности РФ (концепция, стратегии)), информационная безопасность рассматривалась как вид национальной безопасности?
Знать: структуру, задачи и функции органов, регулирующих деятельность объектов и субъектов в сфере ИБ	1.Как, согласно действующему Федеральному закону РФ «О безопасности», принимаются решения Советом безопасности при президенте РФ? 2.Какие органы федеральной государственной исполнительной Федеральными являются регуляторами в сфере надзора за обеспечением безопасности персональных данных в РФ?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если вопросы теста даны полностью или в основном правильные ответы

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если на значительную часть вопросов даны правильны ответы

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если больше чем на половину вопросов даны правильные ответы

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется, если менее чем на половину вопросов даны правильные ответы

КМ-3. Киберпреступления. Основные механизмы противодействия киберпреступности

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Учебная группа. Компьютерный класс. СДО «Прометей». Продолжительность: 1 учебный час

Краткое содержание задания:

Ответить на вопросы теста

Контрольные вопросы/задания:

Знать: обстоятельства возникновения уголовной и административной ответственности при возникновении ИБ-инцидента	1.Какие рекомендации не содержит Будапештская конвенция СЕ по киберпреступности? 2.В каких государствах криминализирован перехват компьютерной информации, включая электромагнитные излучения?
Уметь: определять вид правонарушения в киберсфере и перечень требуемых мер при его выявлении	1.К какому классу киберпреступлений по международной европейской классификации киберпреступлений относится преступление, предусмотренное уголовным законом государства N: «Тот, кто с обманным намерением или с намерением причинить имущественный вред другому лицу, превышает свой доступ к ИТ-системе, наказывается лишением свободы на срок от шести месяцев до трех лет и штрафом от двадцати шести евро до двадцати пяти тысяч евро или только с одним из этих штрафов»? 2.В каком государстве юридически зарегистрирована организация, в случае если в организации возник ИБ-инцидент в виде «Умышленного уничтожения, блокирования, приведения в непригодное состояние компьютерной информации или программы, либо вывода из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж)», и оно квалифицируется компетентными органами государства N как преступление?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если вопросы теста даны полностью или в основном правильные ответы

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если на значительную часть вопросов даны правильны ответы

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если больше чем на половину вопросов даны правильные ответы

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется, если менее чем на половину вопросов даны правильные ответы

КМ-4. Классификация информации по доступу и видам тайн

Формы реализации: Компьютерное задание
Тип контрольного мероприятия: Тестирование

Вес контрольного мероприятия в БРС: 35
Процедура проведения контрольного мероприятия: Учебная группа. Компьютерный класс. СДО «Прометей». Продолжительность: 1 учебный час.

Краткое содержание задания:
Ответить на вопросы теста

Контрольные вопросы/задания:

Знать: принципы правового регулирования информационных отношений	1.Какая информация не относится к информации, которая по нормам 149-ФЗ «Об информации, информационных технологиях и о защите информации» должна быть распространена?
Знать: систему нормативного правового регулирования защиты определённого вида информации и прав её обладателя	1.К какому классу может относиться информация, охраняемая в режиме коммерческой тайны, в классификации информации в зависимости от порядка ее предоставления или распространения, согласно 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
Уметь: использовать правовые нормы для разрешения конфликтов и инцидентов в сфере информационной безопасности	1.Распространение какой информации в информационном поле не запрещено в РФ правовыми нормами? 2.На какие из указанных объектов не распространяются личные имущественные авторские права? 3.Какие из указанных объектов не относятся к объектам авторских прав? 4.Некая компания решила зарегистрировать свой логотип в виде яйца в чёрную и жёлтую полоску на красном фоне. На какие нарушения правомерно указал руководству компании специалист по ИБ?
Уметь: определять необходимые правовые нормы для защиты определённого вида информации и формирования политики безопасности информации и защиты информационных прав субъекта в организации	1.Программист, работающий в организации К, зарегистрированной в РФ, в рамках своих служебных обязанностей разработал компьютерную программу, не имеющую отношение к обороне и не являющуюся предметом государственной тайны, которую компания К в 2021 г. решила продать в КНДР, Афганистан, Иран, Великобританию и США. Будучи законопослушной компанией, руководство обратилось к специалисту по ИБ с распоряжением определить, в какие из предполагаемых отделом маркетинга государства можно правомерно продать программу. Какие именно государства из предложенного перечня в соответствии с требованиями ТРИПС назвал специалист по ИБ как возможные для продажи данной компьютерной программы? 2.Руководитель коммерческой организации К, занимающейся производством детской обуви, формируя перечень информации, подлежащей отнесению в режим коммерческой тайне, включил в данный перечень перечисленные ниже виды информации. Специалист по ИБ указал

	руководителю на то, что один из указанных видов информации не может быть правомерно отнесён к коммерческой тайне. Какой именно вид информации специалист по ИБ рекомендовал изъять из перечня?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если вопросы теста даны полностью или в основном правильные ответы

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если на значительную часть вопросов даны правильны ответы

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если больше чем на половину вопросов даны правильные ответы

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется, если менее чем на половину вопросов даны правильные ответы

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

	Кафедра Безопасности и информационных технологий Дисциплина «Организационно-правовые механизмы обеспечения информационной безопасности» ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1	Утверждаю Зав. кафедрой БИТ А.Н. Невский «22» мая 2024 г. *Протокол №6*

1. Теоретический вопрос. Документы, содержащие официальные взгляды на проблемы информационной безопасности в РФ. Основные положения Доктрины ИБ РФ (2016 г.) и механизмы их реализации.
2. Теоретический вопрос. Порядок отнесения сведений к государственной тайне. Области присутствия информации в режиме государственной тайны. Информация, которая не может быть отнесена к государственной тайне. Сроки засекречивания и порядок рассекречивания информации в режиме государственной тайны в РФ. Уголовная ответственность за нарушение секретности информации, содержащей государственную тайну в РФ.
3. Задача. Коммерческая организация подала заявление о преступлении в ГУ МВД по г. Москве в отношении сотрудника, разгласившего информацию, свободно распространяемую исключительно внутри организации. Объясните, какое решение правомерно должно принять ГУ МВД по г. Москве и почему.
Лектор дисциплины _____ С.Ю. Трофимцева

Процедура проведения

Экзамен проводится в письменной форме в СДО «Прометей» согласно программе экзамена

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-1$_{ОПК-3}$ Организует работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России

Вопросы, задания

1.Государство и его функции в социальной сфере и в сфере безопасности. Формы исполнения функций государством. Обеспечение национальной безопасности как функция государства. Признаки современных государств. Формулы суверенитета.
2.Права человека. Подходы к правам человека. Виды прав человека. Классификация прав человека. Права человека в инфосфере в международной праве и национальном праве России.
3.Нормативный правовой акт: признаки, действие. Нормативные правовые акты РФ по юридической силе в сфере информационной безопасности. Правовая компетенция в

сфере правового регулирования информационной безопасности уровней государственной власти. Документы по стандартизации и их статус в сфере ИБ.
4.Структура правовой нормы. Виды диспозиций. Виды санкций. Структура уголовно-правовых и административно-правовых норм РФ в сфере информационной безопасности.
5.Системы права. Международное право: публичное право, частное право, наднациональное право и их отрасли, регулирующие аспекты информационной безопасности.
6.Национальная правовая система и её характеристика. Элементы правовой системы. Отрасли права, их признаки и отличия. Информационное (цифровое) право. Виды санкций по отраслевой принадлежности.
7.Объекты правоотношений в РФ. Правонарушение. Виды правонарушений. Субъекты правонарушений в сфере информационной безопасности.
8.Уголовное право в сфере регулирования информационной безопасности. Объект преступлений в сфере компьютерной информации в УК РФ. Обстоятельства, исключающие преступность деяния. Виды уголовного преследования по преступлениям в сфере компьютерной информации, по компьютерному мошенничеству, по нарушению прав человека в инфосфере в УК РФ.
9.Административное право в сфере регулирования информационной безопасности. Виды административных наказаний. Административная преюдиция по преступлениям в сфере компьютерной информации в УК РФ.
10.Гражданское право в сфере регулирования информационной безопасности. Объекты гражданских прав. Проблема отнесения информации к объектам гражданских прав в РФ. Подотрасли гражданского права, регулирующие отдельные аспекты информационной безопасности. Основания возникновения гражданских прав и обязанностей в сфере регулирования информационных отношений.
11.Информация как сведения или данные. Правовой статус информации в РФ и в некоторых зарубежных странах. Документированная информация в РФ. Механизмы определения документированности информации
12.Электронный документ и его правовой статус в РФ. Электронная подпись и её виды. Правовое регулирование применения электронной подписи в документообороте организации
13.Охраняемая законом информация в РФ: правовые проблемы. Основные атрибуты статуса защищаемой информации в сфере информационной безопасности. Требования регуляторов (ФСТЭК, ФСБ, РКН, Минцифры)к обеспечению защиты информации в организации
14.Параметры защищаемого статуса информации в ИБ. Информационные отношения и их характеристика. Информация как объект правоотношений: правовые проблемы. Информационное (цифровое) право как комплексное право. Цифровые права в РФ
15.Правовое регулирование информационных отношений. Система нормативного правового обеспечения информационной безопасности. Документы по стандартизации в сфере информационной безопасности и правовой статус их рекомендаций
16.Права человека в информационной сфере и механизмы их обеспечения. Механизмы обеспечения прав сотрудников организации в информационной сфере. Информационная безопасность организации и обеспечение негативных универсальных прав человека в организации
17.Национальная безопасность: содержание и виды. Документы, содержащие официальные взгляды на проблемы национальной безопасности в РФ: трансформация официальных взглядов на проблемы в сфере национальной безопасности. Стратегия национальной безопасности РФ (2021 г.) (основные положения). Стратегические национальные приоритеты в РФ и механизмы их обеспечения

18.Информационная безопасность как вид национальной безопасности. Варианты содержания термина «информационная безопасность». Документы, содержащие официальные взгляды на проблемы информационной безопасности в РФ: трансформация официальных взглядов на проблемы в сфере информационной безопасности. Основные положения Доктрины ИБ РФ (2016 г.) и механизмы их реализации. Составляющие элементы информационной безопасности (варианты). Информационно-психологическая безопасность. Основные виды информационно-психологического воздействия. Механизмы обеспечения информационно-психологической безопасности сотрудников в организации.
19.Структура и функции федеральных органов власти, обеспечивающих информационную безопасность РФ
20.Основные требования к обеспечению безопасности информации в ведомственных нормативных актах федеральных регуляторов в сфере информационной безопасности. Методики классификации нарушителей безопасности информации, виды угроз безопасности информации и их классификация.
21.Генезис киберпреступности и его особенности. Криминализация общественно опасных деяний в киберсреде в национальных правовых системах и современные проблемы эффективного противодействия киберпреступлениям
22.Транснациональная киберпреступность, правовые способы противодействия. Международные документы ООН, СЕ и СНГ: рекомендации по криминализации составов и меры по уголовно-процессуальному противодействию киберпреступности (Будапештская конвенция и Страсбургский протокол СЕ, Модельный кодекс СНГ 1996 г., Душанбинское соглашение СНГ 2018 г., Модельный закон СНГ 2023 г.).
23.Классификация киберпреступлений. Компьютерные преступления и преступления, связанные с компьютерами, в уголовном законодательстве ратификантов Будапештской конвенции, РФ и модельном законодательстве СНГ. Механизмы идентификации киберпреступлений в организациях.
24.Преступления, связанные с содержанием компьютерных данных, их разновидности в РФ. Оконченное и длящееся киберпреступление по российскому уголовному законодательству. Административная и уголовная ответственность за совершение преступления, связанного с содержанием компьютерных данных в РФ. Административная преюдиция по некоторым деяниям.
25.Виды классификации информации по доступу и видам тайн в российском праве. Классификации информации в 149-ФЗ «Об информации, информационных технологиях и о защите информации». Общая классификация информации по доступу и видам тайн в российском праве: основные классы.
26.Информация свободного доступа и свободного распространения: основные виды и правовые требования к её обороту. Правовые проблемы свободного оборота информации в РФ. Виды свободно распространяемой информации и правовые условия их оборота. Механизмы обеспечения оборота свободно распространяемой информации в организациях.
27.Негативная информация: правовые ограничения и запреты её распространения. Виды негативной информации в российском праве. Уголовная и правовая ответственность за распространение негативной информации в РФ. Механизмы противодействия распространению негативной информации в организации и обеспечения информационной безопасности отдельных социальных групп
28.Право интеллектуальной собственности и его составляющие. Правовые проблемы определения прав субъектов на объекты интеллектуальных прав. Уровни правового регулирования защиты объектов интеллектуального права
29.Авторское право. Генезис авторского права в национальных правовых системах. Формирование международной системы защиты авторских прав. Требования международных конвенций и соглашений по защите авторских прав, международное

противодействие распространению контрафакта и «пиратству» (Бернская конвенция 1886 г., Всемирная (Женевская) конвенция по авторскому праву 1952 г., ТРИПС, АСТА, ВОИС)
30.Объекты авторских прав. Понятие страны происхождения объекта авторских прав. Виды авторских прав. Сроки авторских прав. Виды авторского права для группы авторов. Авторские права на сложные объекты авторских прав. Произведения, не являющиеся объектами авторских прав, произведения, не являющиеся объектами исключительных прав. Основные положения ГК РФ (часть IV) по авторскому праву.
31.Субъекты авторских прав. Служебное произведение: механизмы обеспечения прав автора и организации на служебное произведение. Нетрадиционные объекты авторских прав. Механизмы защиты средств индивидуализации организации. Основные положения ГК РФ (часть IV) по авторскому праву
32.Смежные права. Международная и национальная (основные положения ГК РФ (часть IV) по авторскому праву) защита смежных прав. Уголовное и административное наказание за нарушение авторских и смежных прав в РФ. Механизмы соблюдения авторских и смежных прав в организации.
33.Патентное право. Генезис института патентного права. Международная защита патентных прав. Объекты патентных прав. Критерии объектов патентования. Нетрадиционные объекты патентных прав. Основные положения ГК РФ (часть IV) по патентному праву. Международное противодействие нарушению патентных прав (Женевская конвенция 1883 г., ТРИПС, ВТО, ВОИС). Режим фактической монополии в отношении ноу-хау в коммерческих компаниях.
34.Служебный объект патентных прав: механизмы обеспечения прав автора и организации. Условия патентования служебного объекта в РФ.
35.Защищаемая информация, не содержащая тайну: служебная информация ограниченного распространения в РФ. «Чиновничье право». Основные требования к служебной информации ограниченного распространения в РФ. Органы и учреждения, где возможен оборот служебной информации ограниченного распространения в РФ. Требования к носителям служебной информации ограниченного распространения и их хранению. Ответственность за нарушение порядка распространения служебной информации ограниченного распространения в РФ.
36.Служебная тайна в области обороны в РФ. Специфика становления института информации в режиме служебной тайны в РФ. Основные требования к информации в режиме служебной тайны в области обороны в РФ. Требования к носителям информации в режиме служебной тайны в области обороны. Органы и учреждения, где возможен оборот информации в режиме служебной тайны в области обороны в РФ. Ответственность за нарушение порядка распространения информации в режиме служебной тайны в области обороны в РФ.
37.Информация в режиме государственной тайны. Генезис института государственной тайны и ответственности за нарушение режима тайны.
38.Режим государственной тайны в РФ. Основные понятия законодательства РФ по государственной тайне. Принципы отнесения информации к государственной тайне. Реквизиты на носителях, содержащих информацию в режиме государственную тайну. Порядок определения степени секретности информации, содержащей государственную тайну.
39.Порядок отнесения сведений к государственной тайне. Области присутствия информации в режиме государственной тайны. Информация, которая не может быть отнесена к государственной тайне. Сроки засекречивания и порядок рассекречивания информации в режиме государственной тайны в РФ. Уголовная ответственность за нарушение секретности информации, содержащей государственную тайну в РФ
40.Процедура оформления допуска сотрудников к информации в режиме государственной тайны. Требования к организации, проводящей работы с информацией,

содержащей государственную тайну. Перечни информации, содержащей государственную тайну, по законодательству РФ: общая характеристика
41.Информация в режиме коммерческой тайны. Генезис института коммерческой тайны. Информация в режиме коммерческой тайны в зарубежных национальных системах. Международная правовая защита коммерческой тайны (NAFTA, «NAFTA 2.0», GATT, ВТО, ТРИПС).
42.Генезис института коммерческой тайны в России. Основные правовые категории в области коммерческой тайны. Обладатели информации в режиме коммерческой тайны. Права обладателей коммерческой тайны. Обязанности работников коммерческой организации по поддержанию режима коммерческой тайны. Уголовная и административная ответственность за нарушение режима коммерческой тайны
43.Порядок отнесения информации к коммерческой тайне правообладателями. Реквизиты на носителях, содержащих коммерческую тайну в РФ. Базовые требования к режиму коммерческой тайны в коммерческих организациях. Основные документы коммерческой организации по поддержанию режима коммерческой тайны. Правовой порядок разрешения споров между хозяйствующими субъектами по вопросам коммерческой тайны в РФ
44.Информация о частной жизни (личная и семейная тайна). Генезис представлений об приватности части личной информации человека. Становление и эволюция системы правовой защиты частной жизни человека в международном праве. Основные требования по правовым гарантиям защиты частной жизни международных документов
45.Становление института защиты информации частной жизни человека в России. Конституционные права человека в сфере защиты личной и семейной тайны. Ограничения прав человека на защиту частной жизни, личной и семейной тайны в РФ. Правовые нормы законодательства РФ по ограничению права человека на защиту информации о его частной жизни. Особенности запрета на вмешательство в частную жизнь работников для организаций. Тайна коммуникации и правомерность просмотра деловой переписки администраторами ИС в организации: правовые проблемы и механизмы обеспечения
46.Генезис института защиты персональных данных в зарубежном национальном праве. Основные положения международных документов по защите персональных данных. Категории персональных данных в международном праве и требования к трансграничной передаче персональных данных (Страсбургская конвенция 1981 г.).
47.Правовая защита персональных данных в РФ. Принципы защиты персональных данных в РФ. Субъект персональных данных. Понятие избыточности запрашиваемых ПДн. Категории персональных данных в РФ. Правовая и организационная специфика категорий ПДн, объём и содержание каждой категории ПДн
48.Порядок передачи ПДн оператору и порядок отзыва ПДн субъектом. Права и обязанности операторов. Особенности оборота и защиты ПДн в трудовых отношениях. Основные требования к работодателю по защите ПДн работников. Основные документы в организации по защите ПДн. Правовые требования к организации ИСПДн организации. Основные требования регуляторов к защите ИСПДн в организациях
49.Профессиональная тайна. Институт профессиональной тайны в зарубежном национальном праве. Профессиональная тайна в РФ. Виды профессиональных тайн. Режимы профессиональных тайн. Адвокатская тайна, нотариальная тайна, банковская тайна, налоговая тайна, врачебная тайна, тайна журналиста и пр. в РФ. Механизмы защиты информации в режиме профессиональной тайны в РФ.
50.Информация в режиме процессуальной защиты. Требования к обеспечению безопасности информации в режиме процессуальной защиты

Материалы для проверки остаточных знаний

1.К какому виду электронной подписи в российском праве относится квалифицированная электронная подпись?

Ответы:

a. к простой электронной подписи
b. к обычной электронной подписи
c. к усиленной электронной подписи
d. такой подписи в российском праве не существует

Верный ответ: c

2.Какие признаки не относятся к обязательным признакам охраняемой международным правом информации как компьютерных данных?

Ответы:

a. правом информации как компьютерных данных?
b. представление в форме, подходящей для обработки в компьютерной системе
c. представление фактов, сведений или понятий в виде сигналов с использованием компьютерного кода
d. охрана в режиме тайны
e. представление в виде программы, способной обязать компьютерную систему выполнять ту или иную функцию
f. хранение, обработка, передача в информационно-компьютерной системе, находящейся в собственности

Верный ответ: d

3.Откуда, согласно Стратегии национальной безопасности РФ 2021 г., осуществляется большая часть компьютерных атак на российские информационные ресурсы?

Ответы:

a. с территорий иностранных государств
b. с территории Российской Федерации

Верный ответ: a

4.Где криминализирован перехват ПЭМИН, содержащих охраняемую законом компьютерную информацию?

Ответы:

a. во всех государствах - членах СНГ
b. только в России
c. в некоторых государствах Европы и США

Верный ответ: c

5.К какому классу в классификации информации в зависимости от порядка ее предоставления или распространения, согласно 149-ФЗ «Об информации, информационных технологиях и о защите информации» может относиться информация, содержащая специальные персональные данные?

Ответы:

a. информации, свободно распространяемой
b. информации, предоставляемой по соглашению лиц, участвующих в соответствующих отношениях
c. информации, которая в соответствии с федеральными законами подлежит предоставлению или распространению
d. информации, распространение которой в Российской Федерации ограничивается или запрещается

Верный ответ: b, d

6.Составляя форму согласия на обработку персональных данных работника, сотрудник отдела кадров включил в перечень информацию (см. ниже). Специалист по информационной безопасности правомерно указал, что некоторые данные организация

как оператор персональных данных запрашивать не имеет права. Какая информация относится к этим данным?

Ответы:

a. фамилия, имя, отчество
b. дата рождения
c. сведения о состоянии здоровья, профессиональных заболеваниях
d. сведения о деловых и моральных качествах
e. адрес официальной регистрации по месту жительства
f. сведения о составе семьи с указанием фамилий, имён, отчеств лиц, проживающих вместе с работником
g. сведения о доходах по прежним местам работы
h. сведения об образовании, повышении квалификации
i. сведения из свидетельства о смерти

Верный ответ: c, d, f, g, i

7.Какие необходимые реквизиты на носитель, содержащий информацию в режиме коммерческой тайны, правомерно нанёс специалист по информационной безопасности?

Ответы:

a. фамилию, имя, отчество, адрес по месту жительства индивидуального предпринимателя
b. официальное наименование и юридический адрес контрагента
c. перечень лиц, допущенных к этой информации
d. дату отнесения информации к коммерческой тайне
e. дату прекращения режима конфиденциальности
f. гриф «Коммерческая тайна»
g. гриф «Конфиденциально» или «Строго конфиденциально»

Верный ответ: a, d, f

8.Какие из перечисленных прав человека не относятся к негативным правам в информационной сфере?

Ответы:

a. право на получение, хранение и распространение информации
b. свобода совести, включая свободу исповедовать или не исповедовать любую религию
c. право на защиту доброго имени и деловой репутации в суде
d. право на создание средств массовой коммуникации

Верный ответ: c

9.Каким федеральным законом к функциям Совета безопасности при президенте РФ была отнесена функция пресекать призывы к совершению действий, направленных на отчуждение части территории Российской Федерации?

Ответы:

a. была отнесена Федеральным законом «О безопасности» от 28.12.2010 г.
b. содержится в обоих указанных законах
c. не является функцией Совета безопасности

Верный ответ: a

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Оценка "отлично" выставляется, если на вопросы даны полностью или в основном правильные ответы

Оценка: 4
Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Оценка "хорошо" выставляется, если на значительную часть вопросов даны правильны ответы

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется, если больше чем на половину вопросов даны правильные ответы

Оценка: 2
Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется, если менее чем на половину вопросов даны правильные ответы

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.

Для курсового проекта/работы:

2 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

Защита проходит в аудитории в форме доклада, визуализированного презентацией

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Правовые проблемы выявлены, пути их решения определены. Проведён детальный анализ правовых источников. Привлечено и проанализировано значительное количество научной литературы по проблемам работы

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Правовые проблемы в основном выявлены, пути их решения в целом определены, но некоторые правовые вопросы не освящены. Проведён общий анализ правовых источников. Привлечено и проанализировано относительное количество научной литературы по проблемам работы

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Правовые проблемы выявлены частично, пути их решения практически не определены, ряд правовых вопросов не освящен. Анализ правовых источников частичный и поверхностный. Привлечено минимальное количество научной литературы по проблемам работы

Оценка: 2
Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно. Правовые проблемы не выявлены или выявлены незначительно, пути их решения не определены, значительная часть правовых вопросов не освящена. Анализ правовых источников поверхностный или отсутствует. Привлечено минимальное количество научной литературы по проблемам работы или научная литература не привлечена вообще. Работа частично или полностью является компиляцией и / или содержит плагиат.

III. Правила выставления итоговой оценки по курсу

При выставлении итоговой оценки учитывается выполнение графика написания работы, содержание и оформление работы, а также умение студента анализировать нормативные правовые акты и работать с научной литературой по теме.