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

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Организационное и правовое обеспечение информационной безопасности

Москва
2021

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Туркина А.А. Идентификатор: R9001f342-TurkinaAA-3bcc47d9	А.А. Туркина
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

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-1 способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

ИД-1 Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации

2. ОПК-4.1 способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах

ИД-1 Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации

ИД-2 Готовит документы, определяющие правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе

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

ИД-2 Использует нормативные правовые акты в профессиональной деятельности

4. ОПК-8 способен осуществлять подбор, изучение и общение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

ИД-1 Выполняет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

5. ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ИД-1 Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

ИД-2 Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Организация защиты информации на предприятии. Разработка системы защиты информации предприятия (Контрольная работа)
2. Основные функции государственных органов в области информационной безопасности (Контрольная работа)
3. Особенности защиты информации на отдельных объектах информатизации (Семинар)
4. Правовое регулирование отношений в области информации, информационных технологий и защиты информации (Контрольная работа)

Форма реализации: Проверка задания

1. Корпоративная нормативная база по защите информации. Особенности защиты информации при организации электронного документооборота (Кейс (решение конкретных производственных ситуаций))
2. Лицензирование деятельности в области информационной безопасности. Особенности работы с персоналом для обеспечения защиты информации (Семинар)
3. Юридическая ответственность субъектов информационной сферы (Семинар)

Форма реализации: Устная форма

1. Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д. (Мозговой штурм)

БРС дисциплины

3 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства					
Правовое обеспечение информационной безопасности Российской Федерации.		+			
Система права и система законодательства		+			
Основные функции государственных органов в области информационной безопасности		+			
Правовое регулирование отношений в области информации, информационных технологий и защиты информации					
Понятие информации, основы правового регулирования информации в РФ				+	
Основы правового регулирования сети "Интернет" в РФ				+	
Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.					
Законодательство в области государственной тайны.			+		
Правовое регулирование коммерческой тайны и служебной информации ограниченного распространения			+		
Правовое регулирование обработки персональных данных			+		

Особенности защиты отдельных видов профессиональной тайны		+		
Правовое регулирование объектов интеллектуальной собственности и их защита				
Правовое регулирование авторского и смежного права		+		
Правовое регулирование объектов промышленной собственности		+		
Юридическая ответственность субъектов информационной сферы				
Правовое регулирование уголовной ответственности в области информационной безопасности				+
Правовое регулирование административной ответственности в области информационной безопасности				+
Гражданско-правовая и дисциплинарная ответственности в области информационной безопасности				+
Вес КМ:	20	30	30	20

4 семестр

Раздел дисциплины	Веса контрольных мероприятий, %			
	Индекс КМ:	КМ-5	КМ-6	КМ-7	КМ-8
	Срок КМ:	4	8	12	15
Организация защиты информации на предприятии. Разработка системы защиты информации предприятия					
Общая характеристика организации защиты информации на предприятии	+				
Сертификация средств защиты информации	+				
Порядок организации аттестации объектов информатизации	+				
Лицензирование деятельности в области информационной безопасности	+				
Корпоративная нормативная база по защите информации. Политика безопасности					
Особенности работы с персоналом для обеспечения защиты информации				+	
Политика информационной безопасности			+		
Основные организационно-распорядительные документы, определяющие порядок и особенности работы с конфиденциальной информацией на предприятии				+	
Особенности защиты информации при организации электронного документооборота					+
Особенности защиты информации на отдельных объектах информатизации					
Особенности защиты информации при проведении совещаний и переговоров					+
Особенности защиты информации при работе с контрагентами, связанной с передачей конфиденциальной информации					+
Особенности защиты информации на предприятиях топливно-энергетического комплекса					+
Вес КМ:	20	30	30	20	

$Общая часть/Для промежуточной аттестации$

БРС курсовой работы/проекта

4 семестр

Раздел дисциплины	Веса контрольных мероприятий, %		
	Индекс КМ:	КМ-1	КМ-2
	Срок КМ:	8	15
Соблюдение графика выполнения КП/КР		+	
Применение в работе судебной практики и подзаконных нормативных актов			+
	Вес КМ:	50	50

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-1	ИД-1$_{ОПК-1}$ Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Уметь: применять информационные технологии для поиска и обработки информации, в том числе информационно-правовые системы	Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д. (Мозговой штурм)
ОПК-4.1	ИД-1$_{ОПК-4.1}$ Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	Уметь: разрабатывать и участвовать в разработке документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	Корпоративная нормативная база по защите информации. Особенности защиты информации при организации электронного документооборота (Кейс (решение конкретных производственных ситуаций))
ОПК-4.1	ИД-2$_{ОПК-4.1}$ Готовит документы, определяющие правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в	Знать: требования нормативных актов по контролю обеспеченности уровня защищенности информации, содержащейся в	Организация защиты информации на предприятии. Разработка системы защиты информации предприятия (Контрольная работа) Корпоративная нормативная база по защите информации. Особенности защиты информации при организации электронного документооборота (Кейс (решение конкретных производственных ситуаций))

	информационной системе	информационной системе Уметь: применять правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе	
ОПК-5	ИД-2$_{ОПК-5}$ Использует нормативные правовые акты в профессиональной деятельности	Знать: требования нормативных актов в области защиты информации	Основные функции государственных органов в области информационной безопасности (Контрольная работа)
ОПК-8	ИД-1$_{ОПК-8}$ Выполняет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Уметь: выполнять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Юридическая ответственность субъектов информационной сферы (Семинар)
ОПК-10	ИД-1$_{ОПК-10}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению	Знать: требования нормативных актов по формированию политики информационной безопасности Уметь: применять комплексный	Правовое регулирование отношений в области информации, информационных технологий и защиты информации (Контрольная работа) Лицензирование деятельности в области информационной безопасности. Особенности работы с персоналом для обеспечения защиты информации (Семинар)

	информационной безопасности объекта защиты	подход к обеспечению информационной безопасности объекта защиты	
ОПК-10	ИД-2$_{ОПК-10}$ Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации	Уметь: управлять процессом реализации мер защиты информации	Особенности защиты информации на отдельных объектах информатизации (Семинар)

II. Содержание оценочных средств. Шкала и критерии оценивания

3 семестр

КМ-1. Основные функции государственных органов в области информационной безопасности

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Работа проводится в письменном виде, может проводиться очно или с применением ЭО и ДОТ

Краткое содержание задания:
Ответьте на поставленные вопросы с применением нормативно-правовых актов

Контрольные вопросы/задания:

Знать: требования нормативных актов в области защиты информации	1.Назовите основные угрозы информационной безопасности РФ. Каким нормативным актом они предусмотрены? 2.Определите основное значение и цели ФЗ "Об информации, информационных технологиях и защите информации" 3.Укажите основные приоритеты национальной и информационной безопасности Российской Федерации в соответствии с нормативно-правовыми документами в области защиты информации

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ дан верно, допущены небольшие ошибки, в том числе в применении нормативных актов

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Ответы на часть вопросов даны поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы даны поверхностно, или на часть вопросов даны неверные ответы

КМ-2. Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.

Формы реализации: Устная форма
Тип контрольного мероприятия: Мозговой штурм
Вес контрольного мероприятия в БРС: 30

Процедура проведения контрольного мероприятия: Выдается домашнее задание с вопросами по отнесению того или иного вида информации к защищаемым. Результаты домашней подготовки обсуждаются в аудитории. При невозможности обсуждения, работа может быть представлена в письменном виде

Краткое содержание задания:

Определите относится ли рассматриваемая информация к защищемой. Обоснуйте ответ нормами права

Контрольные вопросы/задания:

Уметь: применять информационные технологии для поиска и обработки информации, в том числе информационно-правовые системы	1.Подлежит ли защите Фотография человека / группы лиц 2.Подлежит ли защите информация о переписке человека в социальных сетях 3.Подлежит ли защите информация о текущих затратах предприятия 4.Подлежит ли защите информация об объемах выплаченных организацией налогов и сборов 5.Подлежит ли защите информация о СНИЛС, ФИО, дате рождения работников организации

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ дан верно, допущены небольшие ошибки, в том числе в применении нормативных актов

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Ответы на часть вопросов даны поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы даны поверхностно, или на часть вопросов даны неверные ответы

КМ-3. Правовое регулирование отношений в области информации, информационных технологий и защиты информации

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Работа проводится в письменном виде, может проводиться очно или с применением ЭО и ДОТ

Краткое содержание задания:

Ответьте на поставленные вопросы с применением нормативно-правовых актов

Контрольные вопросы/задания:

Знать: требования нормативных актов по формированию политики информационной безопасности	1.Как осуществляется допуск предприятий и организаций к работе со сведениями, составляющими государственную тайну? Может ли коммерческая организация работать со сведениями составляющими

	государственную тайну? 2.Какие документы необходимо разработать на предприятии для установления режима обработки персональных данных? 3.Какова последовательность действий руководителя предприятия, если предприятие относится к субъектам критической информационной инфраструктуры? Какие критерии учитываются при определении категории объекта?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ дан верно, допущены небольшие ошибки, в том числе в применении нормативных актов

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Ответы на часть вопросов даны поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы даны поверхностно, или на часть вопросов даны неверные ответы

КМ-4. Юридическая ответственность субъектов информационной сферы

Формы реализации: Проверка задания
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Задания выдаются для домашней подготовки. Проверка выполнения может быть в устной форме в виде обсуждения или в письменном виде

Краткое содержание задания:
Рассмотрите ситуацию и подготовьте ответ с использованием нормативно-правовых актов

Контрольные вопросы/задания:

Уметь: выполнять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	1.Панченко и Будин, работали в компьютерной фирме, распространяли «Троянские» программы и получали доступ к паролям пользователей компьютеров. Следствие квалифицировало распространение вирусных программ по ч.1 ст.273 УК РФ, а доступ к чужим паролям по ч.1. ст.272 УК РФ. Дайте анализ объективных и субъективных признаков данных составов преступлений. Решите вопрос о квалификации содеянного. 2.Г., уволенный из автосалона с должности системного администратора, передал за денежное вознаграждение конкурирующей организации базу данных клиентов этого автосалона. Какие виды

	ответственности возможно к нему применить? 3.В., являясь специалистом, а затем менеджером офиса продаж, имея доступ к абонентским контрактам, был уличен в неоднократном сообщении третьим лицам в ходе телефонных переговоров и посредством СМС-сообщений персональных данных абонентов. К какой ответственности он может быть привлечен?

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ дан верно, допущены небольшие ошибки, в том числе в применении нормативных актов

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Ответы на часть вопросов даны поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы даны поверхностно, или на часть вопросов даны неверные ответы

4 семестр

КМ-5. Организация защиты информации на предприятии. Разработка системы защиты информации предприятия

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Работа проводится в письменном виде, может проводиться очно или с применением ЭО и ДОТ

Краткое содержание задания:
Дайте ответы на поставленные вопросы

Контрольные вопросы/задания:

Знать: требования нормативных актов по контролю обеспеченности уровня защищенности информации, содержащейся в информационной системе	1.Для обработки информации конфиденциального характера организация должна получить А) сертификат б) лицензию в) аттестат г) аккредитацию на соответствующий вид деятельности 2.Организация имеет право продолжать использовать для осуществления лицензируемого вида деятельности объект информатизации с установленными на нем средствами защиты после окончания срока действия: а) лицензии б) сертификата

	в) аттестата г) аккредитации

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ дан верно, допущены небольшие ошибки, в том числе в применении нормативных актов

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Ответы на часть вопросов даны поверхностно

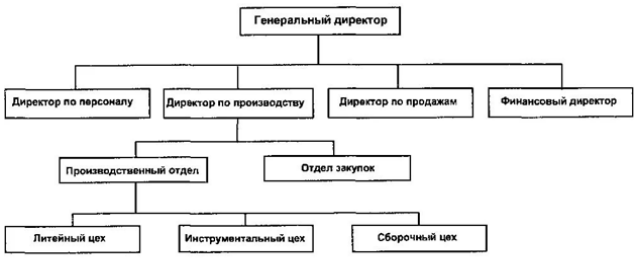
Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы даны поверхностно, или на часть вопросов даны неверные ответы

КМ-6. Лицензирование деятельности в области информационной безопасности. Особенности работы с персоналом для обеспечения защиты информации

Формы реализации: Проверка задания
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Выданное задание может проверяться как в письменном виде, так и в виде обсуждения на семинаре

Краткое содержание задания:
Дайтй ответы на поставленные вопросы

Контрольные вопросы/задания:

Уметь: применять комплексный подход к обеспечению информационной безопасности объекта защиты	1.Определите чем занимается предприятие и где лучше поместить службу ИБ в штатной структуре? Какие требования будут предъявляться к квалификации сотрудника, занимающегося информационной безопасностью?  *Рис. 3. Функциональная организация* 2.Составьте краткую инструкцию по пользованию изделием Генератор шума Покров.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90

Описание характеристики выполнения знания: Ответ дан верно, допущены небольшие ошибки, в том числе в применении нормативных актов

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Ответы на часть вопросов даны поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы даны поверхностно, или на часть вопросов даны неверные ответы

КМ-7. Корпоративная нормативная база по защите информации. Особенности защиты информации при организации электронного документооборота

Формы реализации: Проверка задания
Тип контрольного мероприятия: Кейс (решение конкретных производственных ситуаций)
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Разработайте политику информационной безопасности предприятия исходя из заданных требований

Краткое содержание задания:
По заданному описанию компании и ее производственного процесса разработайте политику информационной безопасности

Контрольные вопросы/задания:

Уметь: разрабатывать и участвовать в разработке документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации	1.По заданному описанию компании и ее производственного процесса разработайте политику информационной безопасности. 1. Компания решила создать филиал в другом городе. Работникам филиала необходимо работать с базой персональных данных, расположенной в головном офисе. Для работы было принято решение использовать VPN-канал, созданный с использованием АПКШ Континент. Разработайте дополнения в политику информационной безопасности компании, касающиеся новой технологии. Объясните работникам филиала и головной организации требования к информационной безопасности. 2.По заданному описанию компании и ее производственного процесса разработайте политику информационной безопасности. 1. Организация принимает решение о создании отдельного переговорного помещения для проведения конфиденциальных переговоров. Разработайте дополнения в политику информационной безопасности компании, касающиеся использования этого помещения. Объясните работникам правила его использования.
Уметь: применять правила и процедуры контроля обеспеченности уровня защищенности информации,	1.По заданному описанию компании и ее производственного процесса разработайте политику информационной безопасности. Организация имеет информационную сеть из 30 рабочих станций и

содержащейся в информационной системе	одного сервера на котором размещена база данных. Для создания резервных копий было принято решение использовать NAS (файловое хранилище). Разработайте дополнения в политику информационной безопасности компании, касающиеся новой технологии. Объясните работникам необходимость создания такого хранилища и правила работы с ним.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ дан верно, допущены небольшие ошибки, в том числе в применении нормативных актов

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Ответы на часть вопросов даны поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы даны поверхностно, или на часть вопросов даны неверные ответы

КМ-8. Особенности защиты информации на отдельных объектах информатизации

Формы реализации: Письменная работа
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 20
Процедура проведения контрольного мероприятия: Результаты выполнения могут быть оценены путем защиты представленных работ или письменные работы

Краткое содержание задания:
Рассмотрите представленные ситуации, определите правомерность действий участников. Предположите, какие меры по защите информации должны были предпринять уучастники, чтобы избежать данной ситуации

Контрольные вопросы/задания:

Уметь: управлять процессом реализации мер защиты информации	1.Рассмотрите представленные ситуации, определите правомерность действий участников. Работник организации А допущенный к персональным данным сотрудников решил использовать их в своих целях. Он обезличил эти персональные данные и использовал в своей книге созданной в свободное время. Другой сотрудник это узнал и требует уволить первого за разглашение персональных данных. Правомерны ли его требования? 2.Рассмотрите представленные ситуации, определите правомерность действий участников. Организация А собирает персональные данные и отправляет их в организацию Б. Организация Б хранит их в облачном хранилище арендуемом у организации В. Хранилище

	находится на сервере организации Г. Кто из перечисленных организаций является оператором персональных данных и кто должен обеспечивать защиту этих данных? 3.Рассмотрите представленные ситуации, определите правомерность действий участников. Червяк Анатолий однажды вечером получил письмо на свой почтовый адрес chervyak@zemlya.ru. "Уважаемый Петр Иванович! Сообщаем Вам, что Вы прикреплены к поликлинике №8. Просим подтвердить: Адрес Вашего проживания: ул.Земляной ком, 15 Полис: №54628910 Адрес эл. Почты: pchervyak@zemlya.ru С уважением, Бухгалтерия поликлиники №8." Анатолий осознал, что бухгалтерия поликлиники ошиблась адресом. И перенаправил данной письмо по требуемому адресу. Предприимчивый червяк Петр, решил, что его пдн были скомпрометированы и решил подать в суд на поликлинику №8 и Анатолия, ведь он мог отправить эти данные всем.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ дан верно, допущены небольшие ошибки, в том числе в применении нормативных актов

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Ответы на часть вопросов даны поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы даны поверхностно, или на часть вопросов даны неверные ответы

Для курсового проекта/работы

4 семестр

I. Описание КП/КР

Получить у преподавателя (руководителя) задание на курсовую работу, ознакомиться с ним и методическими рекомендациями по ее выполнению. Определить, цель, задачи, предмет и объект исследования курсовой работы. Разработать развернутый план курсовой работы, согласно типовой структуры представленной на стр.8. Согласовать план курсовой работы с преподавателем (руководителем). Подобрать и проанализировать учебные материалы

необходимые для разработки курсовой работы. Разработать введение, основную часть и заключение курсовой работы. При необходимости включить в курсовую работу приложения. В случае возникновения в ходе разработки и оформления курсовой работы непонятных вопросов прибыть на индивидуальную консультацию к преподавателю (руководителю).

II. Примеры задания и темы работы

Пример задания

Исследовать правовое регулирование банковской тайны в Российской Федерации и в мировой правктике. Рассматреть особенности регулирования банковской тайны на примере конкреттной организации. Проанализировать судебную практику, связанную с разглашением или установлением некорректного режима банковской тайны. Выявить основные проблемы правового регулирования банковской тайны. Выдвинуть предложения по совершенствованию режима защиты банковской тайны на примере конктретного предприятия или выдвинуть предложения по совершенствованию правового регулирования данного института

Тематика КП/КР:

1. Обзор нормативно-правовых актов по обеспечению защиты информации в организации 2. Основные направления государственной политики России в сфере информационной безопасности 3. Понятие информации и ее виды по порядку организации доступа к ней 4. Основные элементы организационной основы системы обеспечения информационной безопасности России 5. Полномочия в области информационной безопасности и история создания ФСТЭК России. 6. Полномочия в области информационной безопасности и история создания ФСБ России 7. Полномочия МВД России, ФСО России, Службы внешней разведки и Федеральная служба войск национальной гвардии в области информационной безопасности 8. Организация лицензирования деятельности в области защиты информации, осуществляемое ФСТЭК России 9. Организация лицензирования деятельности в области защиты информации, осуществляемое ФСБ России 10. Понятие «коммерческая тайна», особенности ее установления на предприятии 11. Понятие «служебная информация», особенности определения режима её обработки 12. Информация, относимая к секрету производства, особенности ее правовой и организационной защиты 13. Особенности правового регулирования объектов интеллектуальной собственности и порядок их защиты 14. Банковская тайна и порядок ее определения и защиты 15. Профессиональная информация ограниченного доступа и порядок ее защиты 16. Персональные данные и иная личная информация ограниченного доступа и порядок ее защиты 17. Ответственность за нарушение законодательства в сфере защиты информации и особенности ее применения 18. Правовое регулирование применения электронной подписи 19. Понятие и виды электронной подписи, порядок применения электронной подписи во внутреннем (внешнем) документообороте 20. Особенности подтверждения соответствия средств защиты информации установленным нормативным требованиям. 21. Система сертификации средств защиты информации в России 22. Аттестация объектов информатизации, как способ подтверждения соответствия систем установленным требованиям 23. Порядок организации защиты информации на предприятии 24. Особенности разработки положения о пропускном режиме на предприятии 25. Особенности хранения материальных носителей, содержащих информацию ограниченного распространения 26. Организация доступа и допуска персонала к информации ограниченного распространения 27. Особенности защиты информации при проведении совещаний 28. Особенности организации публикации различной информации, на предприятиях, обрабатывающих информацию ограниченного распространения 29. Организация внутриобъектового режима на предприятии 30. Планирование мероприятий по защите информации на предприятии 31. Организация контроля за состоянием защиты информации на предприятии 32. Порядок подключения операторов к Единой

Биометрической Системе (ЕБС) 33. Порядок защиты информации в государственной информационной системе на примере конкретной государственной информационной системы (ГИС) 34. Особенности обработки и защиты персональных данных при создании системы «Умный город» 35. Особенности привлечения к ответственности за киберпреступления в России 36. Правовое регулирования веб-приложений и программного обеспечения, обрабатывающего персональные данные 37. Сравнение законодательства России в области ПДн с европейским GDPR 38. Правовое регулирование интернета в России

КМ-1. Соблюдение графика выполнения КП/КР
Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Первая глава работы предоставлена с соблюдением графика выполнения работы. Первая глава соответствует выданному заданию и действующему законодательству

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Первая глава работы предоставлена с соблюдением графика выполнения работы. Представленный текст не в полном объеме соответствует требованиям задания

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Глава предоставлена с существенным нарушением сроков предоставления. Текст представлен вовремя, но не выполнены требования к качеству текста

КМ-2. Применение в работе судебной практики и подзаконных нормативных актов
Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: В работе предоставлены примеры из судебной практики

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: В работе не все моменты проиллюстрированы примерами из судебной практики. Примеры приведены не всегда верно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Нет примеров из судебной и правоприменительной практики.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

I. Теоретические вопросы:
1. Понятие национальной безопасности, понятие информационной безопасности, в чем заключается их различие
2. Персональные данные и иная личная информация ограниченного доступа

II. Практическое задание
Вправе ли кредитная организация обрабатывать персональные данные физических лиц, получивших отказ в предоставлении кредита? Возможно ли хранить формы анкет-заявок на получение кредита в формате цифровых копий?

Процедура проведения

Устный экзамен. Выдача билета. 15-20 минут самостоятельной подготовки без использования вспомогательных материалов, с возможностью записи краткого конспекта ответа. Ответ на экзаменационные вопросы. Преподаватель может задать уточняющие вопросы по материалам билета.

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

1. Компетенция/Индикатор: ИД-1$_{ОПК-1}$ Понимает значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации

Вопросы, задания

1.Понятие национальной безопасности, понятие информационной безопасности, в чем заключается их различие

Материалы для проверки остаточных знаний

1.Понятие национальной безопасности, понятие информационной безопасности, в чем заключается их различие

Ответы:

Дайте свой ответ

Верный ответ: национальная безопасность Российской Федерации (далее - национальная безопасность) - состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны; Информационная безопасность Российской Федерации (далее - информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое

социально-экономическое развитие Российской Федерации, оборона и безопасность государства. Информационная безопасность является неотъемлемой частью национальной безопасности

2. Компетенция/Индикатор: ИД-2$_{ОПК-5}$ Использует нормативные правовые акты в профессиональной деятельности

Вопросы, задания

1.Источники правового обеспечения информационной безопасности

Материалы для проверки остаточных знаний

1.Источники правового обеспечения информационной безопасности

Ответы:

Дайте свой ответ

Верный ответ: Федеральный закон от 28 декабря 2010 г. N 390-ФЗ "О безопасности“ Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" Указ Президента РФ от 2 июля 2021 г. N 400 "О Стратегии национальной безопасности Российской Федерации" Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" Указ Президента РФ от 9 мая 2017 г. N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы“ Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (Утверждены Президентом Российской Федерации 24 июля 2013 г., № Пр-1753) нормативные акты ФСТЭК, ФСБ и иных уполномоченных в области информационной безопасности

3. Компетенция/Индикатор: ИД-1$_{ОПК-8}$ Выполняет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составляет обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

Вопросы, задания

1.Банковская тайна и иные виды профессиональной информации ограниченного доступа

Материалы для проверки остаточных знаний

1.Банковская тайна и иные виды профессиональной информации ограниченного доступа

Ответы:

Дайте свой ответ

Верный ответ: Статья 857 ГК РФ. Банковская тайна 1. Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. 2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям, а также представлены в бюро кредитных историй на основаниях и в порядке, которые предусмотрены законом. Государственным органам и их должностным лицам, а также иным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, которые предусмотрены законом. 3. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков. Федеральный закон от 02.12.1990 N 395-1 «О банках и банковской деятельности» Федеральный закон от 27 июня 2011 г. N 161-ФЗ "О национальной платежной системе" Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС) Положение Банка России от 9 июня 2012 г. N 382-П "О

требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств« Постановление Правительства от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе»

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ в общем правильный допущены небольшие ошибки в указании нормативных актов, в их применении

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Допущены ошибки не только в наименованиях нормативных актов, но и по правильности их применения. Но в общем ответы на поставленные вопросы даны верно Ответ на один из вопросов билета дан поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы билета даны поверхностно. Отвечающий допустил существенные ошибки в ответе.

III. Правила выставления итоговой оценки по курсу

При формировании итоговой оценки учитывается как результат ответа на экзамене, так и текущая успеваемость студента

4 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

I. Теоретические вопросы:
1. Лицензирование деятельности в области защиты информации, осуществляемое ФСТЭК России, виды лицензий
2. Порядок организации защиты информации на предприятии

II. Практическое задание
Если субъект персональных данных дал согласие на размещение информации о себе в базе коммерческого оператора, а потом передумал. Может ли он потребовать заблокировать ее или вовсе стереть информацию о себе у коммерческого оператора? Что для этого нужно сделать?

Процедура проведения

Устный экзамен. Выдача билета. 15-20 минут самостоятельной подготовки без использования вспомогательных материалов, с возможностью записи краткого конспекта ответа. Ответ на экзаменационные вопросы. Преподаватель может задать уточняющие вопросы по материалам билета.

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

1. Компетенция/Индикатор: ИД-1$_{ОПК-4.1}$ Готовит документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации

Вопросы, задания

1.Аттестация объектов информатизации, как способ подтверждения соответствия систем установленным требованиям

Материалы для проверки остаточных знаний

1.Аттестация объектов информатизации, как способ подтверждения соответствия систем установленным требованиям

Ответы:

Дайте свой вариант ответа

Верный ответ: Аттестация объектов информатизации (далее аттестация) - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Аттестата соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России). Наличие аттестата соответствия в организации дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленный в аттестате. Аттестация является обязательной в следующих случаях: государственная тайна; при защите государственного информационного ресурса; управление экологически опасными объектами; ведение секретных переговоров. Также аттестация проводится в иных случаях, предусмотренных законодательством РФ

2. Компетенция/Индикатор: ИД-2$_{ОПК-4.1}$ Готовит документы, определяющие правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе

Вопросы, задания

1.Планирование мероприятий по защите информации на предприятии

2.Организация контроля за состоянием защиты информации на предприятии

Материалы для проверки остаточных знаний

1.Планирование мероприятий по защите информации на предприятии

Ответы:

Дайте свой вариант ответа

Верный ответ: Действия, которые необходимо запланировать: Обновление прав пользования на средства защиты информации (срочные лицензии) Обновление средств защиты информации (если заканчиваются сертификаты соответствия) Внедрение новых технологий и систем обеспечения ИБ к ним Обновление политики ИБ Обновление иных документов в области ИБ на предприятии Проведение инструктажа на работников предприятия

2.Организация контроля за состоянием защиты информации на предприятии

Ответы:

Дайте свой вариант ответа

Верный ответ: Периодический контроль состояния защищенности аттестованного объекта информатизации осуществляется в процессе эксплуатации и проводится не реже одного раза в год с целью выявления и предотвращения утечки информации по

техническим каналам, исключения или существенного затруднения несанкционированного доступа, а также предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности технических средств, входящих в состав объекта информатизации. В ходе проведения периодического контроля производится оценка: выполнения требований нормативных и методических документов по защите информации; работоспособности и эффективности применяемых средств защиты информации в соответствии с их эксплуатационной документацией с помощью специальной контрольно-измерительной аппаратуры; знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации; актуальности организационно-распорядительных документов по защите информации в организации (изменения в документы должны вноситься в случае увольнения сотрудников, либо перевода их на другое место работы, увеличения числа пользователей на объекте информатизации и других случаях).

3. Компетенция/Индикатор: ИД-1$_{ОПК-10}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

Вопросы, задания

1.Понятие и особенности составления политики информационной безопасности на предприятии

Материалы для проверки остаточных знаний

1.Понятие и особенности составления политики информационной безопасности на предприятии

Ответы:

Дайте свой вариант ответа

Верный ответ: Политика информационной безопасности; политика ИБ: Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации в целом. Политика информационной безопасности; политика ИБ: Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации в целом. Политики бывают: Внутренние – правила поведения для работников предприятия Внешние – декларация для клиентов, лиц чьи персональные данные обрабатываются Полити ксоставляются комиссионно Политики пересматриваются не реже чем один раз в 5 лет.

4. Компетенция/Индикатор: ИД-2$_{ОПК-10}$ Принимает участие в формировании, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управляет процессом их реализации

Вопросы, задания

1. Порядок организации защиты информации на предприятии

Материалы для проверки остаточных знаний

1.Порядок организации защиты информации на предприятии

Ответы:

Дайте свой вариант ответа

Верный ответ: Организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение

конфиденциальной информацией и проявление внутренних и внешних угроз. Организационная защита обеспечивает: – организацию охраны, режима, работу с кадрами, с документами; – использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности. организацию режима и охраны исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 90
Описание характеристики выполнения знания: Ответ в общем правильный допущены небольшие ошибки в указании нормативных актов, в их применении

Оценка: 4
Нижний порог выполнения задания в процентах: 80
Описание характеристики выполнения знания: Допущены ошибки не только в наименованиях нормативных актов, но и по правильности их применения. Но в общем ответы на поставленные вопросы даны верно Ответ на один из вопросов билета дан поверхностно

Оценка: 3
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Ответы на все вопросы билета даны поверхностно. Отвечающий допустил существенные ошибки в ответе.

III. Правила выставления итоговой оценки по курсу

При формировании итоговой оценки учитывается как результат ответа на экзамене, так и текущая успеваемость студента

Для курсового проекта/работы:

4 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

II. Описание шкалы оценивания

Оценка: 5
Нижний порог выполнения задания в процентах: 85
Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

III. Правила выставления итоговой оценки по курсу

При выставлении итоговой оценки учитывается выполнение графика написания работы, содержание и оформление работы, а также качетсов доклада и умение студента аргументированно отстаивать свою точку зрения.