

**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: Очно-заочная

**Оценочные материалы
по дисциплине
Организационное и правовое обеспечение информационной безопасности**

**Москва
2023**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Туркина А.А.
	Идентификатор	R9001f342-TurkinaAA-3bcc47d9

А.А. Туркина

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

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-5 способностью использовать нормативные правовые акты в профессиональной деятельности
2. ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
3. ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности
4. ПК-15 способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
5. ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

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

Форма реализации: Проверка задания

1. Юридическая ответственность субъектов информационной сферы (Семинар)

БРС дисциплины

6 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 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		+			
Особенности защиты отдельных видов информации		+			
Правовое регулирование объектов интеллектуальной собственности и их защита		+			
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			+		
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	+			+
Вес КМ:	25	25	25	25

\$Общая часть/Для промежуточной аттестации\$

БРС курсовой работы/проекта

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %		
	Индекс КМ:	КМ-1	КМ-2
	Срок КМ:	8	15
Соблюдение графика выполнения работы		+	
Использование судебной практики и примеров из практической сферы			+
Вес КМ:		40	60

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-5	ОПК-5(Компетенция)	Знать: нормативные правовые документы по своей профессиональной деятельности; Уметь: использовать нормативные правовые документы в своей профессиональной деятельности;	Основные функции государственных органов в области информационной безопасности (Контрольная работа) Особенности защиты информации на отдельных объектах информатизации (Семинар)
ПК-7	ПК-7(Компетенция)	Знать: теоретические основы обеспечения информационной безопасности на предприятии Уметь: формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и	Правовое регулирование отношений в области информации, информационных технологий и защиты информации (Контрольная работа) Особенности защиты информации на отдельных объектах информатизации (Семинар)

		экономической целесообразности;	
ПК-9	ПК-9(Компетенция)	Знать: виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз; Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью;	Правовое регулирование отношений в области информации, информационных технологий и защиты информации (Контрольная работа)
ПК-15	ПК-15(Компетенция)	Знать: компетенции уполномоченных органов в области информационной безопасности Уметь: организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и	Основные функции государственных органов в области информационной безопасности (Контрольная работа) Юридическая ответственность субъектов информационной сферы (Семинар)

		экспортному контролю; участвовать в работах по реализации политики информационной безопасности	
ОК-4	ОК-4(Компетенция)	Знать: порядок применения норм права Уметь: осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;	Юридическая ответственность субъектов информационной сферы (Семинар)

II. Содержание оценочных средств. Шкала и критерии оценивания

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

Формы реализации: Письменная работа

Тип контрольного мероприятия: Контрольная работа

Вес контрольного мероприятия в БРС: 25

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: нормативные правовые документы по своей профессиональной деятельности;	1. Назовите основные угрозы информационной безопасности РФ. Каким нормативным актом они предусмотрены? 2. Укажите основные приоритеты национальной и информационной безопасности Российской Федерации в соответствии с нормативно-правовыми документами в области защиты информации
Знать: компетенции уполномоченных органов в области информационной безопасности	1. Определите основное значение и цели ФЗ "Об информации, информационных технологиях и защите информации"
Уметь: организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	1. Логически сгруппируйте полномочия ФСТЭК России в соответствии с Указом Президента РФ № 1085

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

Оценка: 2

Описание характеристики выполнения знания: Ответы не предоставлены или предоставлены ответы опирающиеся на недействующее законодательство

КМ-2. 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: 25

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: теоретические основы обеспечения информационной безопасности на предприятии	1. Как осуществляется допуск предприятий и организаций к работе со сведениями, составляющими государственную тайну? Может ли коммерческая организация работать со сведениями составляющими государственную тайну?
Знать: виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз;	1. Какие документы необходимо разработать на предприятии для установления режима обработки персональных данных? 2. Какова последовательность действий руководителя предприятия, если предприятие относится к субъектам критической информационной инфраструктуры? Какие критерии учитываются при определении категории объекта?
Уметь: разрабатывать предложения по совершенствованию системы управления информационной безопасностью;	1. Бывшая сотрудница хлебозавода, воспользовавшись доверительными отношениями с сотрудниками, получила незаконный доступ к компьютеру предприятия, скопировала и распечатала информацию о рецептуре определенной продукции хлебозавода, составляющей коммерческую тайну. Квалифицируйте данные действия.

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

Оценка: 2

Описание характеристики выполнения знания: Ответы не предоставлены или предоставлены ответы опирающиеся на недействующее законодательство

КМ-3. Юридическая ответственность субъектов информационной сферы

Формы реализации: Проверка задания

Тип контрольного мероприятия: Семинар

Вес контрольного мероприятия в БРС: 25

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:

Знать: порядок применения норм права	1.Какой государственный орган привлекает лиц к уголовной ответственности
Уметь: участвовать в работах по реализации политики информационной безопасности	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.
Уметь: осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;	1.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? 2.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

Оценка: 2

Описание характеристики выполнения знания: Ответы не предоставлены или предоставлены ответы опирающиеся на недействующее законодательство

КМ-4. Особенности защиты информации на отдельных объектах информатизации

Формы реализации: Письменная работа

Тип контрольного мероприятия: Семинар

Вес контрольного мероприятия в БРС: 25

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 участники, чтобы избежать данной ситуации

Контрольные вопросы/задания:

Уметь: использовать нормативные правовые документы в своей профессиональной деятельности;	1.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?
Уметь: формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;	1.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

Оценка: 2

Описание характеристики выполнения знания: Ответы не предоставлены или предоставлены ответы опирающиеся на недействующее законодательство

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 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.

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

1. Компетенция/Индикатор: ОПК-5(Компетенция)

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

2. Компетенция/Индикатор: ПК-7(Компетенция)

Вопросы, задания

- 1.Информация, доступ к которой не может быть ограничен
- 2.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

3. Компетенция/Индикатор: ПК-9(Компетенция)

Вопросы, задания

- 1.Понятие и виды электронной подписи
- 2.Понятие «коммерческая тайна», особенности ее установления на предприятии
- 3.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»

4. Компетенция/Индикатор: ПК-15(Компетенция)

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

Политики составляются комиссионно Политики пересматриваются не реже чем один раз в 5 лет.

5. Компетенция/Индикатор: ОК-4(Компетенция)

Вопросы, задания

- 1.Особенности защиты информации на объектах государственных и муниципальных информационных систем
2. 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.

Оценка: 2

Описание характеристики выполнения знания: Студент не дал корректных ответов на поставленные вопросы

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:

6 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты 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

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

Оценка: 2

Описание характеристики выполнения знания: Работа не выполнена или выполнена преимущественно неправильно

III. Правила выставления итоговой оценки по курсу

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