

Аккредитованное образовательное частное учреждение высшего образования
 «Московский финансово-юридический университет МФЮА»
 Информация о владельце:
 ФИО: Забелин Алексей Григорьевич
 Должность: Ректор
 Дата подписания: 02.03.2022 21:01:20
 Уникальный программный ключ:
 672b4d14e1ca30b0f66ad5b6309d064a94afcfdbc652d927620ac07f8fdabb79
 Рассмотрено и одобрено на заседании
 учебно-методического совета

УТВЕРЖДАЮ

Проректор по учебной работе

 В.В. Шутенко
 личная подпись инициалы, фамилия

« 26 » июля 2021 г.

Протокол № 11 от 26.07.2021

Председатель совета

 В.В. Шутенко
 личная подпись инициалы, фамилия

Киселева Светлана Петровна

(уч. звание, степень, ФИО авторов программы)

Рабочая программа дисциплины (модуля)

Правовые основы защиты информации

(наименование дисциплины (модуля))

Направление подготовки (специальность): 09.03.03 Прикладная информатика
 (код, наименование без кавычек)

ОПОП: Прикладная информатика в экономике
 (наименование)

Форма освоения ОПОП: очная, очно-заочная, заочная
 (очная, очно-заочная, заочная)

Общая трудоемкость: 3 (з.е.)

Всего учебных часов: 108 (ак. час.)

Формы промежуточной аттестации	СЕМЕСТР		
	очная	очно-заочная	заочная
Зачет	3	5	5

Москва 2021 г.

Год начала подготовки студентов - 2021

1. Цель и задачи освоения дисциплины

Цель освоения дисциплины	усвоение законодательно-правовых основ правового обеспечения информационной безопасности, принципов построения систем обеспечения информационной безопасности, анализа и оценки угроз информационной безопасности объектов, средств и методов физической защиты объектов, изучение лицензионной и сертификационной деятельности в области защиты информации
Задачи дисциплины	<p>формирование теоретических знаний в области правовых и организационных основ защиты информации, средств и методов защиты информации, построения и организации функционирования систем защиты информации в компьютерных системах, методов несанкционированного доступа и взлома;</p> <p>освоение приемов программной реализации известных криптоалгоритмов и алгоритмов сокрытия информации, защиты системного программного обеспечения;</p> <p>изучение вопросов политики безопасности, стандартов безопасности России и развитых стран;</p> <p>тенденций и перспектив развития средств защиты информации;</p> <p>выработка умения разрабатывать политику безопасности организации, организовать защиту рабочего места, локальной сети.</p>

2. Место дисциплины в структуре ОПОП

Блок 1 «Дисциплины (модули)»	
Дисциплины и практики, знания и умения по которым необходимы как "входные" при изучении данной дисциплины	Правоведение
Дисциплины, практики, ГИА, для которых изучение данной дисциплины необходимо как предшествующее	<p>Защита и обработка конфиденциальных документов</p> <p>Разработка и стандартизация программных средств и информационных технологий</p> <p>Системы искусственного интеллекта</p>

3. Требования к результатам освоения дисциплины

**Компетенции обучающегося, формируемые в результате освоения дисциплины.
Степень сформированности компетенций**

Индикатор	Название	Планируемые результаты обучения	ФОС
УК2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений			
УК-2.1	Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения	Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения	Тест
УК-2.2	Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.	Умеет анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.	Практическое задание

УК-2.3	Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.	Владеет навыками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах	Практическое задание
--------	--	---	----------------------

4. Структура и содержание дисциплины

Тематический план дисциплины

№	Название темы	Содержание	Литература	Индикаторы
1.	Основные понятия в области охраны и защиты информации	<p>Понятие системы права. Понятие и виды защищаемой информации по российскому законодательству.</p> <p>Информация как объект гражданских прав. Виды информации, подлежащие защите в процессе обычного гражданского оборота. Четыре уровня правового обеспечения защиты информации. Характеристика уровней правового обеспечения защиты информации. Категории информации с ограниченным доступом.</p>	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3
2.	Регламентация деятельности по информационной безопасности РФ	<p>Органы законодательства, регламентирующие деятельность по информационной безопасности.</p> <p>Структура органов власти по защите информации в Российской Федерации.</p> <p>Совет Безопасности Российской Федерации.</p> <p>Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации.</p> <p>Федеральная служба безопасности Российской Федерации (ФСБ). Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ). Комитет по вопросам информационной безопасности. Анализ законодательства РФ в области информационной безопасности РФ. Конституционные основы правового обеспечения информационной безопасности РФ. Доктрина информационной безопасности РФ.</p>	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3

3.	Правовое регулирование вопросов в области государственной тайны	<p>Перечень сведений, отнесенных законодателем к категории: государственная тайна по сферам жизнедеятельности общества и государства. Правовой режим защиты государственной тайны. Степени секретности сведений и грифы секретности носителей этих сведений. Органы защиты государственной тайны. Три формы допуска к секретным сведениям. Организация допуска должностных лиц и граждан к государственной тайне. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне. Межведомственная комиссия по защите государственной тайны. Полномочия. Обеспечение деятельности. Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны. Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.</p>	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3
4.	Правовое регулирование вопросов в области остальных видов информации ограниченного доступа	<p>Понятие коммерческой тайны. Правовой режим защиты коммерческой тайны. Требования для классификации сведений категории коммерческой тайны. Понятие банковской тайны. Объекты банковской тайны. Правовой режим защиты банковской тайны. Понятие профессиональной тайны. Требования для классификации сведений категории профессиональной тайны. Объекты профессиональной тайны.</p>	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3

5.	<p>Правовое регулирование вопросов в области конфиденциальной информации</p>	<p>Правовой режим защиты конфиденциальной информации. Понятие служебной тайны. Требования для классификации сведений категории служебной тайны. Перечень сведений, которые не могут быть отнесены к служебной тайне. Понятие персональных данных. Регуляторы в области защиты персональных данных. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Основные объекты интеллектуальной собственности. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области защиты интеллектуальной собственности в области конфиденциальной информации. Уголовная ответственность за правонарушения в области конфиденциальной информации.</p>	<p>9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3</p>	<p>УК-2.1 УК-2.2 УК-2.3</p>
6.	<p>Правовое обеспечение защиты информационных ресурсов</p>	<p>Информационные ресурсы как объект защиты. Классификация информационных ресурсов. Государственные и негосударственные информационные ресурсы. Пользование информационными ресурсами. Системы защиты информационных ресурсов.</p>	<p>9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3</p>	<p>УК-2.1 УК-2.2 УК-2.3</p>

7.	Режим защиты государственных информационных систем	<p>Порядок разработки, согласования и утверждения планов проведения мероприятий по защите государственных информационных систем.</p> <p>Создание и функционирование системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.</p> <p>Стадии и этапы создания системы защиты государственных информационных систем (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).</p> <p>Разработка эксплуатационной документации на систему защиты информации.</p>	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3
8.	Защита критической информационной инфраструктуры	<p>Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ. Меры по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и ее защищенности от компьютерных атак. Правила категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ.</p> <p>Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак.</p>	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3
9.	Аттестация объектов информатизации по требованиям безопасности информации	<p>Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации.</p> <p>Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее – система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по требованиям безопасности информации (добровольная, обязательная). Участники аттестации и их полномочия (компетенции). Задачи, функции права и обязанности органов по аттестации. Деятельность аттестационных комиссий.</p>	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3

10.	Лицензирование и система сертификации средств защиты информации	Организационно-правовые основы лицензирования деятельности по защите информации. Лицензирование деятельности технической и криптографической защите информации. Порядок и методы проведения сертификационных испытаний средств защиты информации основных классов: технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля защищенности информации, программных, аппаратных; средств защиты информации, программных средств контроля защищенности информации. Особенности сертификации средств защиты информации от утечки по техническим каналам. Особенности сертификации средств защиты информации от НСД.	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3
11.	Ответственность за правонарушения в области информационной безопасности РФ	Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области конфиденциальной информации.	9.1.1, 9.2.1, 9.1.2, 9.1.3, 9.1.4, 9.2.2, 9.2.3	УК-2.1 УК-2.2 УК-2.3

Распределение бюджета времени по видам занятий с учетом формы обучения

Форма обучения: очная, 3 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	2	2	0	0	6
2.	4	2	0	2	6
3.	4	2	0	2	6
4.	4	2	0	2	6
5.	3	1	0	2	6
6.	4	2	0	2	6
7.	3	1	0	2	6
8.	3	2	0	1	8
9.	2	1	0	1	6
10.	2	1	0	1	6
11.	3	2	0	1	6
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	36	18	0	16	72

Форма обучения: очно-заочная, 5 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	1	1	0	0	6
2.	3	1	0	2	8
3.	3	1	0	2	8
4.	3	1	0	2	8
5.	3	1	0	2	8
6.	3	1	0	2	8
7.	3	1	0	2	8
8.	2	2	0	0	6
9.	1	1	0	0	6
10.	1	1	0	0	6
11.	1	1	0	0	6
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	26	12	0	12	82

Форма обучения: заочная, 5 семестр

№	Контактная работа	Аудиторные учебные занятия			Самостоятельная работа
		занятия лекционного типа	лабораторные работы	практические занятия	
1.	0	0	0	0	8
2.	2	0	0	2	8
3.	3	1	0	2	8
4.	3	1	0	2	8
5.	3	1	0	2	8
6.	1	1	0	0	8
7.	0	0	0	0	8
8.	0	0	0	0	10
9.	0	0	0	0	8
10.	0	0	0	0	8
11.	0	0	0	0	8
	Промежуточная аттестация				
	2	0	0	0	4
	Консультации				
	0	0	0	0	0
Итого	14	4	0	8	94

5. Методические указания для обучающихся по освоению дисциплины

В процессе освоения дисциплины обучающемуся необходимо посетить все виды занятий, предусмотренные рабочей программой дисциплины и выполнить контрольные задания, предлагаемые преподавателем для успешного освоения дисциплины. Также следует изучить рабочую программу

дисциплины, в которой определены цели и задачи дисциплины, компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения. Рассмотреть содержание тем дисциплины; взаимосвязь тем лекций и практических занятий; бюджет времени по видам занятий; оценочные средства для текущей и промежуточной аттестации; критерии итоговой оценки результатов освоения дисциплины. Ознакомиться с методическими материалами, программно-информационным и материально-техническим обеспечением дисциплины.

Работа на лекции

Лекционные занятия включают изложение, обсуждение и разъяснение основных направлений и вопросов изучаемой дисциплины, знание которых необходимо в ходе реализации всех остальных видов занятий и в самостоятельной работе обучающегося. На лекциях обучающиеся получают самые необходимые знания по изучаемой проблеме. Непременным условием для глубокого и прочного усвоения учебного материала является умение обучающихся сосредоточенно слушать лекции, активно, творчески воспринимать излагаемые сведения. Внимательное слушание лекций предполагает интенсивную умственную деятельность обучающегося. Краткие записи лекций, конспектирование их помогает усвоить материал. Конспект является полезным тогда, когда записано самое существенное, основное. Запись лекций рекомендуется вести по возможности собственными формулировками. Желательно запись осуществлять на одной странице, а следующую оставлять для проработки учебного материала самостоятельно в домашних условиях. Конспект лучше подразделять на пункты, параграфы, соблюдая красную строку. Принципиальные места, определения, формулы следует сопровождать замечаниями. Работая над конспектом лекций, всегда следует использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал лектор.

Практические занятия

Подготовку к практическому занятию следует начинать с ознакомления с лекционным материалом, с изучения плана практических занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. Владение понятийным аппаратом изучаемого курса является необходимым, поэтому готовясь к практическим занятиям, обучающемуся следует активно пользоваться справочной литературой: энциклопедиями, словарями и др. В ходе проведения практических занятий, материал, излагаемый на лекциях, закрепляется, расширяется и дополняется при подготовке сообщений, рефератов, выполнении тестовых работ. Степень освоения каждой темы определяется преподавателем в ходе обсуждения ответов обучающихся.

Самостоятельная работа

Обучающийся в процессе обучения должен не только освоить учебную программу, но и приобрести навыки самостоятельной работы. Самостоятельная работа обучающихся играет важную роль в воспитании сознательного отношения самих обучающихся к овладению теоретическими и практическими знаниями, привитии им привычки к направленному интеллектуальному труду. Самостоятельная работа проводится с целью углубления знаний по дисциплине. Материал, законспектированный на лекциях, необходимо регулярно дополнять сведениями из литературных источников, представленных в рабочей программе. Изучение литературы следует начинать с освоения соответствующих разделов дисциплины в учебниках, затем ознакомиться с монографиями или статьями по той тематике, которую изучает обучающийся, и после этого – с брошюрами и статьями, содержащими материал, дающий углубленное представление о тех или иных аспектах рассматриваемой проблемы. Для расширения знаний по дисциплине обучающемуся необходимо использовать Интернет-ресурсы и специализированные базы данных: проводить поиск в различных системах и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

Подготовка к сессии

Основными ориентирами при подготовке к промежуточной аттестации по дисциплине являются конспект лекций и перечень рекомендуемой литературы. При подготовке к сессии обучающемуся следует так организовать учебную работу, чтобы перед первым днем начала сессии были сданы и защищены все практические работы. Основное в подготовке к сессии – это повторение всего материала курса, по которому необходимо пройти аттестацию. При подготовке к сессии следует весь объем работы распределять равномерно по дням, отведенным для подготовки, контролировать каждый день выполнения работы.

6. Фонды оценочных средств для текущего контроля успеваемости,

промежуточной аттестации и самоконтроля по итогам освоения дисциплины

Технология оценивания компетенций фондами оценочных средств:

- формирование критериев оценивания компетенций;
- ознакомление обучающихся в ЭИОС с критериями оценивания конкретных типов оценочных средств;
- оценивание компетенций студентов с помощью оценочных средств;
- публикация результатов освоения ОПОП в личном кабинете в ЭИОС обучающегося;

Тест для формирования «УК-2.1»

Вопрос №1 .

Согласно Указу Президента РФ от 5 декабря 2016 г. № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" , что информационная безопасность – это

Варианты ответов:

1. совокупность обязательных действий владельца информации
2. состояние защищенности общества и государства, отдельного гражданина от информационно-технического воздействия на информационную инфраструктуру.

Вопрос №2 .

Первый уровень правового обеспечения образуют:

Второй уровень правового обеспечения составляют:

Третий уровень правового обеспечения составляют:

Четвертый уровень правового обеспечения образуют

Тип ответа: Соответствие

Варианты ответов:

1. Первый уровень правового обеспечения образуют:
2. Второй уровень правового обеспечения составляют:
3. Третий уровень правового обеспечения составляют
4. Четвертый уровень правового обеспечения образуют

Варианты соответствий:

1. подзаконные акты
2. локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в КС конкретной организации.
3. государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными
4. международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России.

Вопрос №3 .

Для сохранения конфиденциальных сведений от разглашения используются следующие приемы:

Тип ответа: Многие из многих

Варианты ответов:

1. Сертификация данных
2. Лицензирование
3. Протоколирование
4. Категорирование
5. Аттестация

Вопрос №4 .

Межсетевой экран представляет собой

Варианты ответов:

1. локальное (однокомпонентное) , реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.
2. функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.
3. локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Вопрос №5 .

За нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей предусмотрена

Варианты ответов:

1. Статья 274 УК РФ
2. Статья 274.1 УК РФ
3. Статья 273 УК РФ

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	от 0% до 30% правильных ответов из общего числа тестовых заданий
Удовлетворительно	от 31% до 50% правильных ответов из общего числа тестовых заданий
Хорошо	от 51% до 80% правильных ответов из общего числа тестовых заданий
Отлично	от 81% до 100% правильных ответов из общего числа тестовых заданий

Практическое задание для формирования «УК-2.2»

Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в ситуации: государственный фонд данных государственного экологического мониторинга включает в себя: информацию, содержащуюся в базах данных подсистем единой системы государственного экологического мониторинга; результаты производственного контроля в области охраны окружающей среды и государственного экологического надзора; данные государственного учета объектов, оказывающих негативное воздействие на окружающую среду.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.2»

Определите, соответствуют ли ситуация принципам правового регулирования отношений в сфере информации, информационных технологий и защиты информации: после проведения аудиторской проверки в государственной организации было выявлено нецелевое использование бюджетных средств. Местные средства массовой информации подготовили публикацию об использовании бюджетных средств, однако руководитель организации запретил публиковать данную информацию.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.2»

Проведите анализ информационно-правовой нормы и определите вид формы предписания: Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.2»

Укажите, какой вид электронной подписи должен использоваться при обмене электронными документами между работодателем и дистанционным работником?

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов

Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.2»

Определите, соответствуют ли ситуация принципам правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

На заводе, выпускающем радиоактивные металлы, произошла авария. Возникла реальная опасность радиоактивного заражения, находящегося на расстоянии десяти километров от завода посёлка. Глава местной администрации, опасаясь паники среди населения, запретил до проведения анализа сообщать в средствах массовой информации об аварии.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.3»

Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в ситуации:

юридическое лицо заключило с таможенным представителем договор представлять свои интересы при оформлении таможенной декларации и помещении товаров под определённую таможенную процедуру при перемещении товаров через таможенную границу Таможенного союза, и предоставил ему информацию о себе, товаре и его назначении.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки

Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.3»

Проанализируйте Указ Президента РФ «Об утверждении Перечня сведений конфиденциального характера» и определите, относится ли в представленных примерах информация к конфиденциальной: а) сведения, ставшие известными из телефонных переговоров двух членов семьи о подготовке к семейному торжеству; б) сведения, ставшие известными судебному эксперту при проведении экспертного исследования; в) биографические данные о кандидате в Областную Думу, подготовленные для распространения в средствах массовой информации

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.3»

Физическое лицо обратилось в банк с заявлением о предоставлении кредита. Банку были представлены необходимые сведения о лице: паспортные данные, информация о прописке, сведения о доходах и имуществе. Банк в предоставлении кредита отказал, однако на адрес и телефон заемщика стали поступать предложения от других банков. Какие нарушения прав заемщика были допущены в данном случае банком?

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.3»

В научно-исследовательской лаборатории одного ВУЗа была разработана антикоррозионная присадка защиты корпуса автомобиля от ржавчины. Разработчики не стали подавать заявку на получение патента на изобретение, а решили данную разработку 13 использовать как секрет производства (НОУ-ХАУ) и самостоятельно изготавливать, и продавать присадку потребителям. Какие меры должны быть приняты в данной лаборатории для обеспечения защиты этой разработки. Если аналогичная присадка будет самостоятельно разработана другими лицами, будет ли оставаться данная разработка в режиме коммерческой тайны.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Практическое задание для формирования «УК-2.3»

Центральный банк РФ для анализа экономической ситуации запросил у АО «Тюмень Нефть» информацию о количестве полученной прибыли за прошедший год и о прогнозах объёма добычи нефти на текущий год. Однако АО не предоставило истребуемой информации, мотивировав тем, что информация отнесена к коммерческой тайне. Имеет ли право Банк России получать данную информацию, и несёт ли ответственность Банк России, а также его должностные лица и работники за разглашение коммерческой тайны.

Критерии оценки выполнения задания

Оценка	Критерии оценивания
Неудовлетворительно	Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов
Удовлетворительно	Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки
Хорошо	Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя
Отлично	Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Вопросы для проведения промежуточной аттестации по итогам освоения дисциплины

Тема 1. Основные понятия в области охраны и защиты информации

1. Понятие системы права.
2. Понятие и виды защищаемой информации по российскому законодательству.

3. Информация как объект гражданских прав.
4. Виды информации, подлежащие защите в процессе обычного гражданского оборота.
5. Четыре уровня правового обеспечения защиты информации.
6. Характеристика уровней правового обеспечения защиты информации.
7. Категории информации с ограниченным доступом.

Тема 2. Регламентация деятельности по информационной безопасности РФ

8. Органы законодательства, регламентирующие деятельность по информационной безопасности.
9. Структура органов власти по защите информации в Российской Федерации.
10. Совет Безопасности Российской Федерации.
11. Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации. Федеральная служба безопасности Российской Федерации (ФСБ).
12. Федеральная Служба по техническому и экспортному контролю РФ (ФСТЭК РФ).
13. Комитет по вопросам информационной безопасности.
14. Анализ законодательства РФ в области информационной безопасности РФ.
15. Конституционные основы правового обеспечения информационной безопасности РФ.
16. Доктрина информационной безопасности РФ.

Тема 3. Правовое регулирование вопросов в области государственной тайны

17. Перечень сведений, отнесенных законодателем к категории: государственная тайна по сферам жизнедеятельности общества и государства.
18. Правовой режим защиты государственной тайны.
19. Степени секретности сведений и грифы секретности носителей этих сведений.
20. Органы защиты государственной тайны.
21. Три формы допуска к секретным сведениям.
22. Организация допуска должностных лиц и граждан к государственной тайне.
23. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне.
24. Межведомственная комиссия по защите государственной тайны.
25. Полномочия.
26. Обеспечение деятельности.
27. Социальные гарантии гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны.
28. Порядок проведения специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.

Тема 4. Правовое регулирование вопросов в области остальных видов информации ограниченного доступа

29. Понятие коммерческой тайны.
30. Правовой режим защиты коммерческой тайны.
31. Требования для классификации сведений категории коммерческой тайны.
32. Понятие банковской тайны.
33. Объекты банковской тайны.
34. Правовой режим защиты банковской тайны.
35. Понятие профессиональной тайны.
36. Требования для классификации сведений категории профессиональной тайны. Объекты профессиональной тайны.

Тема 5. Правовое регулирование вопросов в области конфиденциальной информации

37. Правовой режим защиты конфиденциальной информации.
38. Понятие служебной тайны. Требования для классификации сведений категории служебной тайны. Перечень сведений, которые не могут быть отнесены к служебной тайне.
39. Понятие персональных данных. Регуляторы в области защиты персональных данных.
40. Требования к материальным носителям биометрических персональных данных и технологиям

хранения таких данных вне информационных систем персональных данных.

41. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Требования к защите персональных данных при их обработке в информационных системах персональных данных.

42. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

43. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации.

44. Основные объекты интеллектуальной собственности.

45. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации. Меры дисциплинарной ответственности. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности. Уголовная ответственность за правонарушения в области защиты интеллектуальной собственности в области конфиденциальной информации. Уголовная ответственность за правонарушения в области конфиденциальной информации.

Тема 6. Правовое обеспечение защиты информационных ресурсов

46. Информационные ресурсы как объект защиты.

47. Классификация информационных ресурсов.

48. Государственные и негосударственные информационные ресурсы.

49. Пользование информационными ресурсами.

50. Системы защиты информационных ресурсов.

Тема 7. Режим защиты государственных информационных систем

51. Порядок разработки, согласования и утверждения планов проведения мероприятий по защите государственных информационных систем.

52. Создание и функционирование системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.

53. Стадии и этапы создания системы защиты государственных информационных систем (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).

54. Разработка эксплуатационной документации на систему защиты информации.

Тема 8. Защита критической информационной инфраструктуры

55. Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ.

56. Меры по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и ее защищенности от компьютерных атак.

57. Правила категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений.

58. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ.

59. Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

60. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак.

Тема 9. Аттестация объектов информатизации по требованиям безопасности информации

61. Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее – система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

62. Цели аттестации объектов информатизации. Виды аттестации объектов информатизации по

требованиям безопасности информации (добровольная, обязательная).

63. Участники аттестации и их полномочия (компетенции). Задачи, функции права и обязанности органов по аттестации. Деятельность аттестационных комиссий.

Тема 10. Лицензирование и система сертификации средств защиты информации

64. Организационно-правовые основы лицензирования деятельности по защите информации.

65. Лицензирование деятельности технической и криптографической защите информации.

66. Порядок и методы проведения сертификационных испытаний средств защиты информации основных классов: технических средств защиты информации, защищенных технических средств обработки; информации, технических средств контроля защищенности информации, программных, аппаратных; средств защиты информации, программных средств контроля защищенности информации.

67. Особенности сертификации средств защиты информации от утечки по техническим каналам.

68. Особенности сертификации средств защиты информации от НСД.

Тема 11. Ответственность за правонарушения в области информационной безопасности РФ

69. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.

70. Меры дисциплинарной ответственности.

71. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности.

72. Уголовная ответственность за правонарушения в области конфиденциальной информации.

Уровни и критерии итоговой оценки результатов освоения дисциплины

	Критерии оценивания	Итоговая оценка
Уровень 1. Недостаточный	Незнание значительной части программного материала, неумение даже с помощью преподавателя сформулировать правильные ответы на задаваемые вопросы, невыполнение практических заданий	Неудовлетворительно/Незачтено
Уровень 2. Базовый	Знание только основного материала, допустимы неточности в ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Удовлетворительно/зачтено
Уровень 3. Повышенный	Твердые знания программного материала, допустимые несущественные неточности при ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач	Хорошо/зачтено
Уровень 4. Продвинутый	Глубокое освоение программного материала, логически стройное его изложение, умение связать теорию с возможностью ее применения на практике, свободное решение задач и обоснование принятого решения	Отлично/зачтено

7. Ресурсное обеспечение дисциплины

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	<ol style="list-style-type: none"> 1. Microsoft Windows (лицензионное программное обеспечение) 2. Microsoft Office (лицензионное программное обеспечение) 3. Google Chrome (свободно-распространяемое программное обеспечение) 4. Браузер Спутник (свободно-распространяемое программное обеспечение отечественного производства) 5. Kaspersky Endpoint Security (лицензионное программное обеспечение) 6. «Антиплагиат.ВУЗ» (лицензионное программное обеспечение)
Современные профессиональные базы данных	<ol style="list-style-type: none"> 1. Консультант+ (лицензионное программное обеспечение отечественного производства) 2. http://www.garant.ru (ресурсы открытого доступа)
Информационные справочные системы	<ol style="list-style-type: none"> 1. https://elibrary.ru - Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа) 2. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа) 3. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа) 4. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)
Интернет-ресурсы	<ol style="list-style-type: none"> 1. http://window.edu.ru - Информационная система "Единое окно доступа к образовательным ресурсам" 2. https://openedu.ru - «Национальная платформа открытого образования» (ресурсы открытого доступа)
Материально-техническое обеспечение	<p>Учебные аудитории для проведения:</p> <p>занятий лекционного типа, обеспеченные наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации, помещения для хранения и профилактического обслуживания учебного оборудования.</p>

8. Учебно-методические материалы

№	Автор	Название	Издательство	Год издания	Вид издания	Кол-во в библиотеке	Адрес электронного ресурса	Вид доступа
1	2	3	4	5	6	7	8	9
9.1 Основная литература								
9.1.1	Ельчанинова Н.Б.	Правовые основы защиты информации с ограниченным доступом	Издательство Южного федерального университета	2017	учебное пособие	-	http://www.iprbookshop.ru/87470.html	по логину и паролю
9.1.2	Петренко В.И.	Теоретические основы защиты информации	Северо-Кавказский федеральный университет	2015	учебное пособие	-	http://www.iprbookshop.ru/63138.html	по логину и паролю
9.1.3	Гулятьева Т.А.	Основы защиты информации	Новосибирский государственный технический университет	2018	учебное пособие	-	http://www.iprbookshop.ru/91638.html	по логину и паролю

9.1.4	Исаев А.С. Хлюпина Е.А.	Правовые основы организации защиты персональных данных	Университет ИТМО	2014	учебное пособие	-	http://www.iprbookshop.ru/67564.html	по логину и паролю
9.2 Дополнительная литература								
9.2.1	Шаньгин В.Ф.	Защита компьютерной информации. Эффективные методы и средства	Профобразование	2019	учебное пособие	-	http://www.iprbookshop.ru/87992.html	по логину и паролю
9.2.2	Ефимова Л.Л.	Правовые основы информатики	Евразийский открытый институт	2011	учебное пособие	-	http://www.iprbookshop.ru/11069.html	по логину и паролю
9.2.3	Башлы П.Н. Бабаш А.В. Баранова Е.К.	Информационная безопасность и защита информации	Евразийский открытый институт	2012	учебное пособие	-	http://www.iprbookshop.ru/10677.html	по логину и паролю

9. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья

В МФЮА созданы специальные условия для получения высшего образования по образовательным программам обучающимися с ограниченными возможностями здоровья (ОВЗ).

Для перемещения инвалидов и лиц с ограниченными возможностями здоровья в МФЮА созданы специальные условия для беспрепятственного доступа в учебные помещения и другие помещения, а также их пребывания в указанных помещениях с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

При получении образования обучающимся с ограниченными возможностями здоровья при необходимости предоставляются бесплатно специальные учебники и учебные пособия, иная учебная литература. Также имеется возможность предоставления услуг ассистента, оказывающего обучающимся с ограниченными возможностями здоровья необходимую техническую помощь, в том числе услуг сурдопереводчиков и тифлосурдопереводчиков.

Получение доступного и качественного высшего образования лицами с ограниченными возможностями здоровья обеспечено путем создания в университете комплекса необходимых условий обучения для данной категории обучающихся. Информация о специальных условиях, созданных для обучающихся с ограниченными возможностями здоровья, размещена на сайте университета (<http://www.mfua.ru/sveden/objects/#objects>).

Для обучения инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата обеспечиваются и совершенствуются материально-технические условия беспрепятственного доступа в учебные помещения, столовую, туалетные, другие помещения, условия их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и др.).

Для адаптации к восприятию обучающимися инвалидами и лицами с ОВЗ с нарушенным слухом справочного, учебного материала, предусмотренного образовательной программой по выбранным направлениям подготовки, обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы, оповещающие о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагог смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих инвалидов и лиц с ОВЗ проводится за счет:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;

- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию инвалидами и лицами с ОВЗ с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой МФЮА по выбранной специальности, обеспечиваются следующие условия:

ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;

в начале учебного года обучающиеся несколько раз проводятся по зданию МФЮА для запоминания месторасположения кабинетов, помещений, которыми они будут пользоваться;

педагог, его собеседники, присутствующие представляются обучающимся, каждый раз называется тот, к кому педагог обращается;

действия, жесты, перемещения педагога коротко и ясно комментируются;

печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;

обеспечивается необходимый уровень освещенности помещений;

предоставляется возможность использовать компьютеры во время занятий и право записи объяснения на диктофон (по желанию обучающегося).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ определяется преподавателем в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ с учетом его индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.