Автономная некоммерческая образовательная организация
высшего образования
«Воронежский экономико-правовой институт»
(АНОО ВО «ВЭПИ»)

АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ

Подписано цифровой подписью: АНОО ВО "ВОРОНЕЖСКИЙ ЭКОНОМИКО-ПРАВОВОЙ ИНСТИТУТ", АНОО ВО "ВЭПИ", ВЭПИ
Дата: 2021.12.21 11:49:08 +03'00'

УТВЕРЖДАЮ
Проректор
по учебно-методической работе
_____ А.Ю. Жильников
«20» декабря 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Б1.В.11 Правовые основы информационной безопасности
(наименование дисциплины (модуля))

40.03.01 Юриспруденция
(код и наименование направления подготовки)

Направленность (профиль) Уголовно-правовая
(наименование направленности (профиля))

Квалификация выпускника Бакалавр
(наименование квалификации)

Форма обучения Очная, очно-заочная, заочная
(очная, очно-заочная, заочная)

Рекомендован к использованию филиалами АНОО ВО «ВЭПИ»

Воронеж 2021

Фонд оценочных средств по дисциплине (модулю) рассмотрен и одобрен на заседании кафедры Юриспруденции.

Протокол от «__12__» _____ноября_____ 2021__ г. № 4

Фонд оценочных средств по дисциплине (модулю) согласован со следующими представителями работодателей или их объединений, направление деятельности которых соответствует области профессиональной деятельности, к которой готовятся обучающиеся:

1. И.о. руководителя УФССП России по Воронежской области – Главного судебного пристава Воронежской области Р.Н. Паринов

(должность, наименование организации, фамилия, инициалы, подпись, дата, печать)

2. Заведующий адвокатской консультацией № 2 Ленинского района г. Воронежа Ю.Ф. Закурдаев

(должность, наименование организации, фамилия, инициалы, подпись, дата, печать)

Заведующий кафедрой А.М. Годовникова

Разработчики:

Доцент А.Н. Богомолов

1. Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО

Целью проведения дисциплины Б1.В.11 Правовые основы информационной безопасности является достижение следующих результатов обучения:

Код компетенции	Наименование компетенции
ПК-2	Способен обеспечивать соблюдение законодательства Российской Федерации субъектами права

В формировании данных компетенций также участвуют следующие дисциплины (модули), практики образовательной программы (по семестрам (курсам) их изучения):

- для очной формы обучения:

Наименование дисциплин (модулей), практик	Этапы формирования компетенций по семестрам изучения							
	1 сем.	2 сем.	3 сем.	4 сем.	5 сем.	6 сем.	7 сем.	8 сем.
Гражданское право			ПК-2	ПК-2	ПК-2	ПК-2		
Экологическое право				ПК-2				
Земельное право			ПК-2					
Финансовое право					ПК-2			
Налоговое право						ПК-2		
Международное частное право								ПК-2
Семейное право					ПК-2			
Прокурорский надзор							ПК-2	
Уголовно-исполнительное право					ПК-2			
Наследственное право							ПК-2	
Право интеллектуальной собственности								ПК-2
Жилищное право					ПК-2			
Гражданско-правовая ответственность							ПК-2	
Банковское право								ПК-2
Административный процесс			ПК-2					
Правовое регулирование сделок с недвижимым имуществом			ПК-2					
Таможенное право				ПК-2				
Корпоративное право				ПК-2				
Гражданское население в противодействии распространению идеологии терроризма								ПК-2
Учебная практика (ознакомительная практика)				ПК-2				
Производственная практика (правоприменительная практика)						ПК-2		
Производственная практика (преддипломная практика)								ПК-2

- для очно-заочной формы обучения:

Наименование дисциплин (модулей), практик	Этапы формирования компетенций по семестрам изучения									
	1 сем.	2 сем.	3 сем.	4 сем.	5 сем.	6 сем.	7 сем.	8 сем.	9 сем.	А сем.
Гражданское право			ПК-2	ПК-2	ПК-2	ПК-2				
Экологическое право					ПК-2					
Земельное право					ПК-2					
Финансовое право							ПК-2			
Налоговое право							ПК-2			
Международное частное право										ПК-2
Семейное право						ПК-2				
Прокурорский надзор								ПК-2		
Уголовно-исполнительное право							ПК-2			
Наследственное право									ПК-2	
Право интеллектуальной собственности								ПК-2		
Жилищное право							ПК-2			
Гражданско-правовая ответственность									ПК-2	
Банковское право									ПК-2	
Административный процесс					ПК-2					
Правовое регулирование сделок с недвижимым имуществом					ПК-2					
Таможенное право						ПК-2				
Корпоративное право						ПК-2				
Гражданское население в противодействии распространению идеологии терроризма								ПК-2		
Учебная практика (ознакомительная практика)						ПК-2				
Производственная практика (правоприменительная практика)								ПК-2		
Производственная практика (преддипломная практика)										ПК-2

- для заочной формы обучения:

Наименование дисциплин (модулей), практик	Этапы формирования компетенций по курсам изучения				
	1 курс	2 курс	3 курс	4 курс	5 курс
Гражданское право		ПК-2	ПК-2		
Экологическое право			ПК-2		
Земельное право			ПК-2		
Финансовое право			ПК-2		
Налоговое право				ПК-2	
Международное частное право					ПК-2

Семейное право				ПК-2	
Прокурорский надзор					ПК-2
Уголовно-исполнительное право				ПК-2	
Наследственное право					ПК-2
Право интеллектуальной собственности					ПК-2
Жилищное право				ПК-2	
Гражданско-правовая ответственность					ПК-2
Банковское право					ПК-2
Административный процесс			ПК-2		
Правовое регулирование сделок с недвижимым имуществом			ПК-2		
Таможенное право			ПК-2		
Корпоративное право			ПК-2		
Гражданское население в противодействии распространению идеологии терроризма					ПК-2
Учебная практика (ознакомительная практика)			ПК-2		
Производственная практика (правоприменительная практика)				ПК-2	
Производственная практика (преддипломная практика)					ПК-2

Этап дисциплины (модуля) Б1.В.11 Правовые основы информационной безопасности в формировании компетенций соответствует:

- для очной формы обучения – 6 семестру;
- для очно-заочной формы обучения – семестр А;
- для заочной формы обучения – 5 курсу.

2. Показатели и критерии оценивания компетенций на различных этапах их формирования, шкалы оценивания

Показателями оценивания компетенций являются следующие результаты обучения:

Код компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)
ПК-2	ИПК-2.1. Знает правовые формы реагирования на выявленные факты нарушения российского законодательства.	Знать основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности.
	ИПК-2.2. Владеет способами защиты прав.	Уметь анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности
	ИПК-2.3. Выявляет взаимосвязь требований законодательства и правоприменительной практики.	Владеть навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины (модуля):

№ п/п	Наименование раздела дисциплины (модуля)	Код компетенции, код индикатора достижения компетенции	Критерии оценивания	Оценочные средства текущего контроля успеваемости	Шкала оценивания
1	Тема 1. Предмет и система дисциплины «Правовые основы информационной безопасности»	ПК-2 (ИПК-2.3)	Владеет навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере	Устный опрос, решение задач, реферат, доклад	Зачтено; не зачтено
2	Тема 2. Понятие, признаки, классификация информации и принципы правового регулирования отношений в сфере информации	ПК-2 (ИПК-2.1, ИПК-2.2)	Знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности Умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности	Устный опрос, решение задач, реферат, доклад	Зачтено; не зачтено
3	Тема 3. Понятие, задачи и сферы обеспечения информационной	ПК-2 (ИПК-2.1)	Знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий,	Устный опрос, решение задач, реферат, доклад, круглый стол,	Зачтено; не зачтено

	безопасности		категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности	тестирование	
4	Тема 4. Правовые институты, обеспечивающие защиту информации	ПК-2 (ИПК-2.2)	Умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности	Устный опрос, решение задач, реферат, доклад, тестирование	Зачтено; не зачтено
5	Тема 5. Уголовно-правовые меры борьбы и криминологическая характеристика преступлений, посягающих на охраняемую законом информацию	ПК-2 (ИПК-2.2.)	Умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности	Устный опрос, решение задач, реферат, доклад, круглый стол, тестирование	Зачтено; не зачтено
6	Тема 6. Организационные методы защиты информации	ПК-2 (ИПК-2.2.)	Умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности	Устный опрос, решение задач, реферат, доклад, тестирование	Зачтено; не зачтено
ИТОГО			Форма контроля	Оценочные средства промежуточной аттестации	Шкала оценивания
			зачет с оценкой	Вопросы к зачету с оценкой	«отлично», «хорошо», «удовле-творительно», «неудовле-творительно»

Критерии оценивания результатов обучения для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

1. Критерии оценивания устного ответа.

- зачтено – знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности; умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности; владеет навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере;

- не зачтено – не выполнены требования, соответствующие оценке «зачтено».

2. Критерии оценивания реферата.

- зачтено – знает основные положения отраслевых юридических и

специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности; умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности; владеет навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере;;

- не зачтено – не выполнены требования, соответствующие оценке «зачтено».

3. Критерии оценивания доклада.

- зачтено – знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности; умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности; владеет навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере;;

- не зачтено – не выполнены требования, соответствующие оценке «зачтено».

4. Критерии оценивания тестирования.

- зачтено – знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности; умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности; владеет навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере;

- не зачтено – не выполнены требования, соответствующие оценке «зачтено».

5. Критерии оценивания решения задач.

- зачтено – знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности; умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности; владеет навыками реализации норм материального и процессуального права; навыками принятия необходимых

мер защиты прав человека и гражданина в информационной сфере;

- не зачтено – не выполнены требования, соответствующие оценке «зачтено».

5. Критерии оценивания ответа на зачете с оценкой.

«Отлично»

Знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности.

Умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности.

Владеет навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере.

«Хорошо»:

- в целом знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности;

- в целом умеет анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности;

- в целом владеет навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере.

«Удовлетворительно»:

- не достаточно хорошо знает основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов, правоотношений в сфере информационной безопасности;

- не достаточно хорошо анализировать юридические факты и возникающие в связи с ними правовые отношения в сфере обеспечения информационной безопасности;

- не достаточно хорошо навыками реализации норм материального и процессуального права; навыками принятия необходимых мер защиты прав человека и гражданина в информационной сфере.

«Неудовлетворительно»:

- не выполнены требования, соответствующие оценке «отлично», «хорошо», «удовлетворительно».

3. Типовые контрольные задания или иные материалы, необходимые

для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций
1 ЭТАП

«Текущий контроль успеваемости»

Тема 1. Предмет и система дисциплины «Правовые основы информационной безопасности»

Вопросы:
1. Понятие и предмет дисциплины.
2. Система, основные понятия дисциплины
3. Источники дисциплины «Правовые основы информационной безопасности».

Темы докладов:
1. Информационное общество.
2. Информационные процессы в современном обществе и их значение.

Темы рефератов:
1. Понятие информации и смежные с ним понятия.
2. Понятие и правовая природа информационного общества.

Задачи:

Выбирая в магазине средство для ухода за изделиями из кожи, гражданин Смирновобратился за консультацией к продавцу, который посоветовал ему купить средство «GLE- DIS» (страна изготовитель Германия).

Также продавец рассказал о преимуществах данного средства и о том, как его необходимо использовать. Выслушав продавца, Смирнов приобрел указанное средство.

Придя домой, и собираясь использовать приобретенный товар Смирнов решил ознакомиться с инструкцией по его применению, но обнаружил, что вся инструкция написана только на немецком языке. Смирнов не владел знанием немецкого языка и побоялся использовать средство, дабы не испортить дорогой кожаный диван.

Смирнов вернулся в магазин и попросил у продавца инструкцию к «GLEDIS» на русском языке, но продавец, сказал, что инструкция на русском языке к данному средству отсутствует, но так как он свободно владеет немецким языком, предложил Смирнову зачитать прилагавшуюся к средству инструкцию.

Смирнов возмутился и заявил, что живет в России и в услугах переводчика не нуждается, тем более не знает ли продавец в действительности немецкий язык или нет, а так же не уверен в

достоверности того перевода который тот сделает. В связи с чем, Смирнов решил вернуть товар и вернуть потраченные на его приобретение деньги.

В удовлетворении данного требования руководство магазина Смирнову отказало. Возмущенный Смирнов решил данное дело так не оставлять и обратился в суд за защитой своих интересов.

Нарушено ли право Смирнова на информацию?

Возможна ли на территории Российской Федерации продажа непродовольственных товаров без информации о них на Русском языке?

Составьте от лица Смирнова жалобу на действия администрации магазина. Составьте мотивированное решение суда по жалобе Смирнова.

Тема 2. Понятие, признаки, классификация информации и принципы правового регулирования отношений в сфере информации

Вопросы:

1. Основные теоретические и законодательные подходы к определению термина «информация».
2. Классификация информации по различным основаниям.
3. Принципы правового регулирования отношений в сфере информации.

Темы докладов:

1. Понятие и виды информации.
2. Классификация видов информации.
3. Особенности документированной информации как объекта правовой охраны.

Темы рефератов:

1. Понятие правового режима информации и его разновидности
2. Информационная политика государства.

Задачи:

Работник Конструкторского бюро Сергеев, имея определенные знания в области оружейного дела, разработал устройство, имеющее поражающее действие, которое собирался использовать для охоты. Обратившись в уполномоченный федеральный орган для регистрации устройства в качестве изобретения, ему указали на то, что данное устройство подлежит изъятию и засекречиванию.

Какие права и обязанности возникают у Сергеева в данной ситуации согласно Закону РФ «О государственной тайне»?

Тема 3. Понятие, задачи и сферы обеспечения информационной безопасности

Вопросы:

1. Понятие информационной безопасности.
2. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Национальные интересы России в информационной сфере.
3. Задачи обеспечения информационной безопасности.
4. Классификация угроз информационной безопасности.
5. Понятие «информационной войны» и «информационного оружия».

Занятия в интерактивной форме проводятся в форме круглого стола «Информационная безопасность в сети Интернет»

Темы докладов:

1. Значение информационной безопасности для обеспечения национальных интересов России на современном этапе развития общества.
2. Проблемы обеспечения информационной безопасности в экономической сфере.
3. Идеологическая безопасность и проблемы негативного влияния информации на массовое сознание.
4. История и современность информационных войн.

Темы рефератов:

1. Сущность права на информационную безопасность и его гарантии.
2. Система законодательства об информационной безопасности.

Задачи:

Двое бывших сотрудников компании «ЛАДА», воспользовавшись паролем администратора, удалили с сервера компании файлы, составлявшие крупный (на несколько миллионов

долларов) проект иностранного заказчика. К счастью, имелась резервная копия проекта, так

что реальные потери были незначительны.

Разберите приведенную ситуацию и определите:

- что является источником угрозы информационной безопасности;
- какой в данном случае вид угрозы информационной безопасности (например, внутренняя или внешняя);
- чьи интересы в информационной сфере в данной ситуации страдают?

Подлежат ли действия бывших сотрудников компании «ЛАДА» ответственности в

соответствии с действующим законодательством Российской Федерации?

Тестирование:

Задание № 1

Понятие «информационная безопасность» закреплено

1. в Законе Российской Федерации от 27 декабря 1991 г. №1224-11 «О средствах массовой информации»;

2. в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3. в Доктрине информационной безопасности Российской Федерации

Задание № 2

Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства

1. угроза информационной безопасности;
2. предполагаемые действия иностранных государств;
3. деятельность иностранных разведок.

Тема 4. Правовые институты, обеспечивающие защиту информации

Вопросы:

1. Понятие тайны как социального и правового института, обеспечивающего защиту информации. Виды тайн.
2. Нормативно-правовое регулирование института государственной тайны.
3. Конфиденциальная информация: понятие, виды, особенности правового статуса.

Темы докладов:

Социальный и правовой феномен тайны.

Государственная тайна: история и современность.

Особенности правового регулирования институтов коммерческой и служебной тайн.

Профессиональная тайна как объект правовой защиты.

Темы рефератов:

1.Принципы формирования сведений, составляющих государственную тайну.

2.Соотношение государственной и служебной тайн.

3.Правовой режим коммерческой тайны.

4.Правовой режим персональных данных.

Задачи:

К руководителю НИИ «Магнит» Ермакову обратился начальник отдела по работе со сведениями, составляющими государственную тайну Семенов с необходимостью определения степени секретности информации, полученной в опытной лаборатории НИИ. Ермаков, ознакомившись с данной информацией и с Перечнем сведений, составляющих государственную тайну, разработанным в НИИ и не обнаружив в Перечне полученной в лаборатории

информации, указал Семенову ничего не предпринимать и ждать очередной проверки соответствующими органами.

Проанализируйте эту ситуацию с точки зрения норм Закона РФ «О государственной тайне»

Тестирование:

Задание № 1

Процедура оформления права граждан на доступ к сведени¬ям, составляющим государственную тайну, — это

1. конституционное право гражданина;
2. обязательная процедура;
3. допуск к государственной тайне.

Задание № 2

Информация, относящаяся к прямо или косвенно определенному или определяемому лицу является

1. персональными данными субъекта;
2. коммерческой тайной;
3. служебной тайной.

Тема 5. Уголовно-правовые меры борьбы и криминологическая характеристика преступлений, посягающих на охраняемую законом информацию

Вопросы:

1. Понятие и классификация преступлений, посягающих на охраняемую законом информацию.
2. Уголовная политика государства в информационной сфере.
3. Криминологическая характеристика преступлений, посягающих на охраняемую законом информацию.
4. Уголовно-правовые меры борьбы с преступлениями, связанными с разглашением охраняемых законом тайн (ст. ст. 137, 138, 155, 183, 275, 276, 283, 284, 310, 311, 320 УК РФ).
5. Преступления, должностных лиц в сфере информационных отношений (ст. ст. 140, 237, 287 УК РФ).
6. Компьютерная информация - объект уголовно-правовой охраны (ст. ст. 271-273 УК РФ).

Занятия в интерактивной форме проводятся в форме круглого стола

Круглый стол «Уголовно-правовые меры борьбы с преступлениями, посягающими на охраняемую законом информацию»

Понятие преступлений, посягающих на охраняемую законом информацию.

Классификация информационных преступлений. Уголовная политика государства в информационной сфере.

Уголовно-правовые меры борьбы с преступлениями, связанными с разглашением охраняемых законом тайн (ст. ст. 137, 138, 155, 183, 275, 276, 283, 284, 310, 311, 320 УК РФ).

Преступления, должностных лиц в сфере информационных отношений (ст. ст. 140, 237, 287 УК РФ). Компьютерная информация – объект уголовно-правовой охраны (ст. ст. 272-274 УК РФ).

Темы докладов:

1. Проблемы квалификации преступлений в сфере компьютерной информации.
2. Особенности правовой оценки криминальных деяний, посягающих на информационную безопасность в экономической сфере.
3. «Информационный» преступник: личностный портрет.
4. Роль правоохранительных органов в профилактике и предупреждении преступлений, посягающих на охраняемую законом информацию.

Темы рефератов:

1.Правонарушения в информационной сфере: понятие, виды, состав.

2.Уголовная ответственность за преступления в информационной сфере.

3.Киберпреступления: понятие, основные черты и формы проявления.

Задачи:

Левченко и другие граждане Российской Федерации вступили в сговор на похищение денежных средств в крупных размерах, принадлежащих "City Bank of America", расположенного в г. Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 2007 г., используя электронную компьютерную систему телекоммуникационной связи "Интернет" и преодолев при этом несколько рубежей многоконтурной защиты от несанкционированного доступа с помощью персонального компьютера стандартной конфигурации из офиса предприятия, находящегося в г. Санкт-Петербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате этих операций было осуществлено не менее 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка на счета лиц, входящих в состав преступной группы, проживающих в шести странах: США, Великобритании, Израиле, Швейцарии, ФРГ, России.

Дайте уголовно-правовую оценку действиям Левченко и других членов организованной группы.

Тестирование:

Задание № 1
Предметом информационных преступлений является

1. документированная информация;
2. любая информация;
3. сведения (сообщения, данные) независимо от формы их предоставления;
4. конфиденциальная информация.

Задание № 2
Видовым объектом преступлений в сфере компьютерной информации являются

1. права и интересы физических и юридических лиц, общества и государства по поводу использования автоматизированных систем обработки данных;
2. безопасность информации и систем обработки информации с использованием эвм;
3. специфическая группа общественных отношений - информационные отношения, содержание которых составляют права и интересы различных субъектов в области функционирования информационной техники и использования компьютерной информации, необходимой для их нормальной жизнедеятельности;
4. общественные отношения по безопасному производству информации с помощью ЭВМ.

Тема 6. Организационные методы защиты информации

Вопросы:
1. Система государственных и негосударственных органов обеспечивающих защиту информации.
2. Организационные методы зашиты информации.
3. Режим секретности или конфиденциальности.
4. Порядок рассекречивания информации.
5. Лицензирование в области защиты информации.

Темы докладов:
1. Организационно-правовые меры защиты служебной информации в госучреждениях.
2. Соблюдение режима коммерческой тайны как элемент экономической безопасности фирмы.
3. «Обратный инжиниринг» как способ добывания коммерчески полезной информации.

Темы рефератов:

1. Деятельность служб экономической безопасности по предотвращению утечек информации.

2. «Обратный инжиниринг» как способ добывания коммерчески полезной информации.

Задачи:

Определите значение лицензированию и сертификации в области обеспечения информационной безопасности. Какие виды деятельности в Российской Федерации подлежат лицензированию в целях обеспечения информационной безопасности личности, общества, государства?

Тестирование:

Задание № 20

Какой бывает информация по категории доступа

1. открытая и закрытая;
2. общедоступная и с ограниченным доступом;
3. закрытая и с ограниченным доступом;
4. засекреченная и общедоступная.

Примерный перечень тем рефератов по дисциплине «Правовые основы информационной безопасности»

1. Понятие информации и смежные с ним понятия.
2. Понятие правового режима информации и его разновидности.
3. Информационная политика государства.
4. Сущность права на информационную безопасность и его гарантии.
5. Система законодательства об информационной безопасности.
6. Понятие и правовая природа информационного общества.
7. Обеспечение информационной безопасности личности.
8. Обеспечение информационной безопасности государства.
9. Объективная и субъективная стороны информационной безопасности.
10. Правоотношения в сфере информационной безопасности (понятие, виды, элементы).
11. Правонарушения в информационной сфере: понятие, виды, состав.
12. Гражданско-правовая ответственность за правонарушения в информационной сфере.
13. Административно-правовая ответственность за правонарушения в информационной сфере.
14. Уголовная ответственность за преступления в информационной сфере.

15.Киберпреступления: понятие, основные черты и формы проявления.

16.Принципы формирования сведений, составляющих государственную тайну.

17.Соотношение государственной и служебной тайн.

18.Правовое регулирование международного информационного обмена.

19.Соотношение служебной и коммерческой тайн.

20.Правовое регулирование использования аналогов собственноручной подписи.

21.Правовой режим коммерческой тайны.

22.Правовой режим персональных данных.

23.Правовая защита информации.

24.Право граждан на доступ к информации.

25.Право юридических лиц на получение информации.

2 ЭТАП «Промежуточная аттестация по итогам освоения дисциплины»

Вопросы для подготовки к зачету с оценкой по дисциплине «Правовые основы информационной безопасности»

1. Понятие и предмет дисциплины «Правовые основы информационной безопасности».
2. Система, основные понятия и источники дисциплины «Правовые основы информационной безопасности».
3. Основные теоретические и законодательные подходы к определению термина «информация».
4. Виды созданной и производной правовой информации, их краткая характеристика.
5. Понятие информационных ресурсов, информационных продуктов, документированной информации.
6. Свойства информации.
7. Классификация информации по различным основаниям.
8. Особенности правовой защиты объектов интеллектуальной собственности.
9. Информационные процессы в современном обществе и их значение.
10. Особенности документированной информации как объекта правовой охраны.
11. Понятие информационной безопасности.
12. Структура законодательства об информационной безопасности.

13. Содержание и значение Стратегии национальной безопасности Российской Федерации до 2020 года от 12 марта 2009 г. № 537.
14. Содержание и значение Федерального закона «Об информации, информационных технологиях, и о защите информации» 27 июля 2006 г. № 149-ФЗ.
15. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.
16. Национальные интересы России в информационной сфере.
17. Задачи обеспечения информационной безопасности.
18. Классификация угроз информационной безопасности.
19. Понятие «информационной войны» и «информационного оружия».
20. Общая характеристика конституционно-правовых норм, регулирующих отношения по обеспечению информационной безопасности.
21. Соотношение понятий «информационная безопасность» и «безопасность информации».
22. Объекты мероприятий по обеспечению информационной безопасности.
23. Понятие тайны как социального и правового института, обеспечивающего защиту информации.
24. Классификация тайн.
25. Нормативно-правовое регулирование института государственной тайны.
26. Содержание и значение Закона РФ от 21 июня 1991 г. № 5485-1 «О государственной тайне».
27. Принципы засекречивания информации.
28. Рассекречивание информации: порядок и основания.
29. Порядок и правила распоряжения информацией, составляющей государственную тайну.
30. Конфиденциальная информация: понятие и виды.
31. Тайна частной жизни.
32. Тайна следствия и судопроизводства.
33. Служебная тайна.
34. Профессиональная тайна.
35. Коммерческая тайна и ноу-хау.
36. Промышленный шпионаж: понятие и проблемы противодействия.
37. Понятие и общая характеристика преступлений, посягающих на охраняемую законом информацию.
38. Уголовная политика государства в информационной сфере.
39. Уголовно-правовые меры борьбы с преступлениями, связанными с разглашением охраняемых законом тайн (ст.ст. 137, 138, 155, 183, 275, 276, 283, 284, 310, 311, 320 УК РФ).
40. Преступления, должностных лиц в сфере информационных отношений (ст.ст. 140, 237, 287 УК РФ).
41. Компьютерная информация - объект уголовно-правовой охраны (ст.ст. 272-274 УК РФ).

42. Основные детерминанты преступности, связанной с посягательствами на охраняемую законом информацию.
43. Криминологическая характеристика личности преступника, посягающего на охраняемую законом информацию.
44. Профилактика и предупреждение преступлений, посягающих на охраняемую законом информацию.
45. Роль ОВД в профилактике и предупреждении преступлений, посягающих на охраняемую законом информацию.
46. Система государственных и негосударственных органов обеспечивающих защиту информации.
47. Организационные методы зашиты информации.
48. Режим секретности или конфиденциальности.
49. Порядок рассекречивания информации.
50. Лицензирование в области защиты информации.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

I этап –текущий контроль успеваемости

На первом этапе обучающийся планирует свою самостоятельную работу, которая включает:

уяснение задания на самостоятельную работу;

решение задач по темам;

подбор рекомендованной литературы;

составление плана работы, в котором определяются основные пункты предстоящей подготовки.

Составление плана дисциплинирует и повышает организованность в работе.

Второй этап включает непосредственную подготовку обучающегося к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной

литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы обучающийся должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале.

Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым вопросам.

В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь.

При необходимости следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

Требования к подготовке реферата

Реферат - краткое изложение содержания документа или его части, научной работы, включающее основные фактические сведения и выводы, необходимые для первоначального ознакомления с источниками и определения целесообразности обращения к ним.

Современные требования к реферату - точность и объективность в передаче сведений, полнота отображения основных элементов, как по содержанию, так и по форме.

Цель реферата - не только сообщить о содержании реферируемой работы, но и дать представление о вновь возникших проблемах соответствующей отрасли науки.

В учебном процессе реферат представляет собой краткое изложение в письменном виде или в форме публичного доклада содержания книги, учения, научного исследования и т.п. Иначе говоря, это доклад на определенную тему, освещающий её вопросы на основе обзора литературы и других источников.

Подготовка и написание реферата. При написании реферата необходимо следовать следующим правилам:

Раскрытие темы реферата предполагает наличие нескольких источников (как минимум 4-5 публикаций, монографий, справочных изданий, учебных пособий) в качестве источника информации.

Подготовка к написанию реферата предполагает внимательное изучение каждого из источников информации и отбор информации непосредственно касающейся избранной темы. На этом этапе работы важно выделить существенную информацию, найти смысловые абзацы и ключевые слова, определить связи между ними.

Содержание реферата ограничивается 2-3 параграфами (§§).

Сведение отобранной информации непосредственно в текст реферата, должно быть выстроено в соответствии с определенной логикой. Реферат состоит из трех частей: введения, основной части, заключения.

Во введении логичным будет обосновать выбор темы реферата, актуальность (почему выбрана данная тема, каким образом она связана с современностью?); цель (должна соответствовать теме реферата); задачи (способы достижения заданной цели), отображаются в названии параграфов работы; историография (обозначить использованные источники с краткой аннотаций – какой именно источник (монография, публикация и т.п.), основное содержание вцелом (1 абз.), что конкретно содержит источник по данной теме (2-3 предложения).

В основной части дается характеристика и анализ темы реферата в целом, и далее – сжатое изложение выбранной информации в соответствии с поставленными задачами. В конце каждой главы должен делаться вывод (подвывод), который начинается словами: «Таким образом…», «Итак…», «Значит…», «В заключение главы отметим…», «Все сказанное позволяет сделать вывод…», «Подводя итог…» и т.д. Вывод содержит краткое заключение по §§ главы (объем 0,5–1 лист). В содержании не обозначается.

Заключение содержит те подвыводы по параграфам, которые даны в работе (1-1,5 листа). Однако прямая их переписка нежелательна; выгодно смотрится заключение, основанное на сравнении. Например, сравнение типов политических партий, систем, идеологий и др. Уместно высказать свою точку зрения на рассматриваемую проблему.

Список литературы. В списке указываются только те источники, на которые есть ссылка в основной части реферата. Ссылка в основном тексте оформляется:

В подстрочнике: цитата выделяется кавычками, затем следует номер ссылки. Нумерация ссылок на каждой странице начинается заново. Например, **«Цитата…»** [1].

Библиографическое описание книги в списке использованной литературы оформляется в соответствии с ГОСТ, (фамилия, инициалы автора, название работы, город издания, издательство, год издания, общее количество страниц).

При использовании материалов из сети ИНТЕРНЕТ необходимо оформить ссылку на использованный сайт.

Тематика рефератов разрабатывается преподавателем дисциплины и предоставляется обучающимся заранее либо самим преподавателем, либо методистом соответствующей кафедры (через старост). С темами рефератов можно ознакомиться в пункте 12.3.

Реферат выполняется на листах формата А4 в компьютерном варианте. Поля: верхнее, нижнее – 2 см, правое – 3 см, левое – 1,5 см, шрифт Times New Roman, размер шрифта – 14, интервал – 1,5, абзац – 1,25, выравнивание по ширине. Объем реферата 15-20листов. Нумерация страниц обязательна.

Номер страницы ставится по центру вверху страницы. ***Титульный лист*** не нумеруется.

Рефераты сдаются преподавателю в указанный срок. Реферат не будет зачтен в следующих случаях:

1. Существенных нарушений правил оформления (отсутствует содержание или список литературы, нет сносок, номеров страниц и т.д.).
2. Серьезных недостатков в содержании работы (несоответствие структуры работы ее теме, неполное раскрытие темы, использование устаревшего фактического материала).

Возвращенный обучающемуся реферат должен быть исправлен в соответствии с рекомендациями преподавателя. Обучающийся, не получивший зачет по реферату, к зачету с оценкой не допускается.

Требования к подготовке доклада

Доклад - вид самостоятельной работы, используется в учебных заведениях, способствует формированию навыков исследовательской работы, расширяет познавательные интерес, приучает критически мыслить.

При написании доклада по заданной теме составляют план, подбирают основные источники. В процессе работы с источниками систематизируют полученные сведения, делают выводы и обобщения. К докладу по крупной теме могут, привлекаться несколько обучающихся, между которыми распределяются вопросы выступления.

В настоящее время доклады, по содержанию практически ничем не отличаются от рефератов, и является зачетной работой обучающегося.

Отличительными признаками доклада являются:

- передача в устной форме информации;
- публичный характер выступления;
- стилевая однородность доклада;
- четкие формулировки и сотрудничество докладчика и аудитории;
- умение в сжатой форме изложить ключевые положения исследуемого вопроса и сделать выводы.

Подготовка к выполнению тестового задания

При подготовке к выполнению тестового задания необходимо внимательно изучить структуру теста, оценить объем времени, выделяемого на данный тест, увидеть, какого типа задания в нем содержатся. Это поможет настроиться на работу.

Лучше начинать отвечать на те вопросы, в правильности решения которых нет сомнений, пока не останавливаясь на тех, которые могут вызвать долгие раздумья. Это позволит успокоиться и сосредоточиться на выполнении более трудных вопросов.

Очень важно всегда внимательно читать задания до конца, не пытаясь понять условия «по первым словам» или выполнив подобные задания в

предыдущих тестированиях. Такая спешка нередко приводит к досадным ошибкам в самых легких вопросах.

Если вы не знаете ответа на вопрос или не уверены в правильности, следует пропустить его и отметить, чтобы потом к нему вернуться.

Важно думать только о текущем задании. Как правило, задания в тестах не связаны друг с другом непосредственно, поэтому необходимо концентрироваться на данном вопросе и находить решения, подходящие именно к нему. Кроме того, выполнение этой рекомендации даст еще один психологический эффект – позволит забыть о неудаче в ответе на предыдущий вопрос, если таковая имела место.

Многие задания можно быстрее решить, если не искать сразу правильный вариант ответа, а последовательно исключать те, которые явно не подходят. Метод исключения позволяет в итоге сконцентрировать внимание на одном-двух вероятных вариантах.

Рассчитывать выполнение заданий нужно всегда так, чтобы осталось время на проверку и доработку (примерно 1/3-1/4 запланированного времени). Тогда вероятность описок сводится к нулю и имеется время, чтобы набрать максимум баллов на легких заданиях и сосредоточиться на решении более трудных, которые вначале пришлось пропустить.

Процесс угадывания правильных ответов желательно свести к минимуму, так как это чревато тем, что обучающийся забудет о главном: умении использовать имеющиеся накопленные в учебном процессе знания, и будет надеяться на удачу. Если уверенности в правильности ответа нет, но интуитивно появляется предпочтение, то психологи рекомендуют доверять интуиции, которая считается проявлением глубинных знаний и опыта, находящихся на уровне подсознания.

При подготовке к тесту не следует просто заучивать материал, необходимо понять логику изложенного материала. Этому немало способствует составление развернутого плана, таблиц, схем, внимательное изучение исторических карт. Положительным результатом тестирования можно считать 50-100% правильных ответов.

II этап – промежуточная аттестация по итогам освоения дисциплины

Зачет с оценкой - это форма оценки усвоения учебного материала дисциплин (разделов дисциплин), а также выполнения программ практик.

Зачеты с оценкой принимаются преподавателями, проводившими практические занятия в группе, или лекторами потока.

Результаты прохождения промежуточной аттестации для дисциплин, по которым в соответствии с учебным планом предусмотрена форма контроля «зачет с оценкой», оцениваются отметками:

- «отлично» - обучающийся полно и аргументировано отвечает по содержанию задания; обнаруживает понимание материала, может обосновать

свои суждения, применить знания на практике, привести необходимые примеры не только по учебнику, но и самостоятельно составленные; излагает материал последовательно и правильно;

- «хорошо» - обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «отлично», но допускает 1-2 ошибки, которые сам же исправляет;

- «удовлетворительно» - ставится, если обучающийся обнаруживает знание и понимание основных положений данного задания, но: излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки;

- «неудовлетворительно» - обучающийся обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал; отмечаются такие недостатки в подготовке обучающегося, которые являются серьезным препятствием к успешному овладению последующим материалом.

5. Материалы для компьютерного тестирования обучающихся в рамках проведения контроля наличия у обучающихся сформированных результатов обучения по дисциплине

Общие критерии оценивания

№ п/п	Процент правильных ответов	Оценка
1	86 % – 100 %	5 («отлично»)
2	70 % – 85 %	4 («хорошо)
3	51 % – 69 %	3 (удовлетворительно)
4	50 % и менее	2 (неудовлетворительно)

Вариант 1

Номер вопроса и проверка сформированной компетенции

№ вопроса	Код компетенции	№ вопроса	Код компетенции	№ вопроса	Код компетенции	№ вопроса	Код компетенции

1	ПК-2 ПК-8	6	ПК-2 ПК-8	11	ПК-2 ПК-8	16	ПК-2 ПК-8
2	ПК-2 ПК-8	7	ПК-2 ПК-8	12	ПК-2 ПК-8	17	ПК-2 ПК-8
3	ПК-2 ПК-8	8	ПК-2 ПК-8	13	ПК-2 ПК-8	18	ПК-2 ПК-8
4	ПК-2 ПК-8	9	ПК-2 ПК-8	14	ПК-2 ПК-8	19	ПК-2 ПК-8
5	ПК-2 ПК-8	10	ПК-2 ПК-8	15	ПК-2 ПК-8	20	ПК-2 ПК-8

Ключ ответов

№ вопроса	верный ответ	№ вопроса	верный ответ	№ вопроса	верный ответ	№ вопроса	верный ответ
1	2	6	3	11	1	16	3
2	3	7	3	12	3	17	3
3	3	8	1	13	3	18	1
4	2	9	3	14	2	19	4
5	1	10	3	15	1	20	3

Задание № 1
Согласно легальному определению информация - это

1. сведения о каких-либо событиях, явлениях, процессах, передаваемые от человека к человеку
2. сведения (сообщения, данные) независимо от формы их представления
3. сообщение, переданное или полученное пользователем информационно-телекоммуникационной сети

Задание № 2
Под киберпреступлением понимается

1. самостоятельный вид виновно совершенного общественно опасного деяния, запрещенного нормами Уголовного кодекса Российской Федерации
2. любое преступление, совершенное в сфере информационной безопасности
3. совершение действий в системе Интернет, при которых компьютер является орудием либо предметом посягательства в кибернетическом пространстве

Задание № 3
Понятие «информационная безопасность» закреплено

1. в Законе Российской Федерации от 27 декабря 1991 г. №1224-11 «О средствах массовой информации»;
2. в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. в Доктрине информационной безопасности Российской Федерации.

Задание № 4
Коммерческая тайна представляет собой

1. защищаемые юридическим лицом сведения любого характера (производственные, технические, экономические), имеющие коммерческую ценность в силу неизвестности их третьим лицам;
2. режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;
3. сведения, для которых установлен специальный режим сбора, хранения, обработки, распространения и использования, доступ к которым ограничен в соответствии с федеральным законом.

Задание № 5
Обладателем секрета производства является

1. лицо, которое использует ноу-хау в целях извлечение прибыли;
2. лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании;
3. любое юридическое лицо или индивидуальный предприниматель.

Задание № 6
Информация в электронной форме, которая присоединена к другой информации в электронной форме или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию – это

1. ключ электронной подписи;
2. сертификат ключа проверки электронной подписи;
3. электронная подпись.

Задание № 7
Документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации

1. секретная информация;
2. информация, зафиксированная на специальном носителе;
3. конфиденциальная информация.

Задание № 8

Перечень сведений, составляющих государственную тайну, определяется

1. Федеральным законом;
2. Указом Президента;
3. Постановлением Правительства.

Задание № 9

Основные преступления в информационной сфере перечислены в Уголовном кодексе Российской Федерации в главе

1. 11;
2. 18;
3. 28.

Задание № 10

Процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, — это

1. конституционное право гражданина;
2. обязательная процедура;
3. допуск к государственной тайне.

Задание № 11

Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства

1. угроза информационной безопасности;
2. предполагаемые действия иностранных государств;
3. деятельность иностранных разведок.

Задание № 12

Не являются видами угроз информационной безопасности:

1. внутренние угрозы;
2. внешние угрозы;
3. значительные угрозы.

Задание № 13

Состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства

1. обеспечение безопасного использования информации;
2. состояние безопасного информационного обмена;
3. информационная безопасность.

Задание № 14

К методам обеспечения информационной безопасности Российской Федерации относятся

1. методы принуждения;
2. организационно-технические;
3. секретные.

Задание № 15

Информация, относящаяся к прямо или косвенно определенному или определяемому лицу является

1. персональными данными субъекта;
2. коммерческой тайной;
3. служебной тайной.

Задание № 16

Лицо, самостоятельно создавшее информацию, либо получившее право разрешать или ограничивать доступ к информации, является

1. создателем информации;
2. хранителем информации;
3. обладателем информации.

Задание № 17

Информационная безопасность это

1. состояние защищенности информационной среды общества, обеспечивающее ее использование и развитие в интересах граждан, организаций, государства;
2. состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз;
3. 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;
4. состояние защищенности государства.

Задание № 18
В политической сфере объектами защиты в рамках обеспечения информационной безопасности выступают

1. сведения, составляющие государственную и служебную тайну, конфиденциальные сведения корпоративного характера;
2. общественное сознание;
3. собственность граждан;
4. сведения, составляющие личную, семейную тайну.

Задание № 19
Характерным признаком тайны являются

1. круг лиц, которым известны или доверены сведения, составляющие тайну не должен быть ограничен;
2. сведения (информация) не должны обладать ценностью для конкретного социального субъекта;
3. разглашение этих сведений влечет наступление только дисциплинарной ответственности;
4. сведения не подлежат разглашению вообще, или в течение определенного срока, установленного законом или внутриведомственным (внутриорганизационным) актом.

Задание № 20
Конфиденциальность информации это

1. служебная тайна;
2. сведения, составляющие тайну следствия и судопроизводства;
3. обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
4. сведения о сущности изобретения, полезной модели или промышленного образца после официальной публикации информации о них.

Вариант 2

Номер вопроса и проверка сформированной компетенции

№ вопроса	Код компетенции	№ вопроса	Код компетенции	№ вопроса	Код компетенции	№ вопроса	Код компетенции

1	ПК-2 ПК-8	6	ПК-2 ПК-8	11	ПК-2 ПК-8	16	ПК-2 ПК-8
2	ПК-2 ПК-8	7	ПК-2 ПК-8	12	ПК-2 ПК-8	17	ПК-2 ПК-8
3	ПК-2 ПК-8	8	ПК-2 ПК-8	13	ПК-2 ПК-8	18	ПК-2 ПК-8
4	ПК-2 ПК-8	9	ПК-2 ПК-8	14	ПК-2 ПК-8	19	ПК-2 ПК-8
5	ПК-2 ПК-8	10	ПК-2 ПК-8	15	ПК-2 ПК-8	20	ПК-2 ПК-8

Ключ ответов

№ вопроса	верный ответ	№ вопроса	верный ответ	№ вопроса	верный ответ	№ вопроса	верный ответ
1	3	6	1	11	1	16	2
2	3	7	2	12	3	17	3
3	2	8	1	13	3	18	4
4	3	9	4	14	1	19	1
5	2	10	1	15	1	20	2

Задание № 1
Предметом информационных преступлений является

1. документированная информация;
2. любая информация;
3. сведения (сообщения, данные) независимо от формы их предоставления;
4. конфиденциальная информация.

Задание № 2
Видовым объектом преступлений в сфере компьютерной информации являются

1. права и интересы физических и юридических лиц, общества и государства по поводу использования автоматизированных систем обработки данных;
2. безопасность информации и систем обработки информации с использованием эвм;
3. специфическая группа общественных отношений - информационные отношения, содержание которых составляют права и интересы различных субъектов в области функционирования информационной техники и использования компьютерной информации, необходимой для их нормальной жизнедеятельности;

4. общественные отношения по безопасному производству информации с помощью ЭВМ.

Задание № 3

К действиям по неправомерному доступу к охраняемой законом компьютерной информации относятся

1. похищение компьютера;
2. всякая форма проникновения к ней с использованием средств (вещественных и интеллектуальных) электронно-вычислительной техники, позволяющая манипулировать информацией (уничтожать ее, блокировать, модифицировать, копировать);
3. завладение любым машинным носителем информации как вещью;
4. уничтожение, блокирование, модификация либо копирование информации.

Задание № 4

К модификации компьютерной информации не следует относить

1. любые изменения компьютерной информации, затрудняющие работу законного пользователя;
2. частичной замены первоначальной информации на другую;
3. уничтожение компьютерных файлов;
4. добавление новой компьютерной информации к первоначальной.

Задание № 5

К органам призванным обеспечивать информационную безопасность России не следует относить

1. федеральную службу безопасности;
2. федеральную службу исполнения наказаний;
3. межведомственную комиссию по защите государственной тайны;
4. министерство цифрового развития, связи и массовых коммуникаций российской федерации.

Задание № 6

Под уничтожением информации следует понимать

1. изменение ее состояния, при котором утрачивается возможность ее восприятия извне кем бы то ни было;
2. любые изменения компьютерной информации, затрудняющие работу законного пользователя;
3. перемещение оригинальной компьютерной информации на машинный носитель или другой компьютер, с условием удаления ее с компьютера потерпевшего;
4. частичную замену первоначальной информации на другую.

Задание № 7
Способом совершения преступления, предусмотренного ст. 183 УК «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», является

1. собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов;
2. собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом;
3. собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем анализа опубликованной в открытой печати информации;
4. разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, с согласия их владельца.

Задание № 8
Документированная информация это

1. зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством российской федерации случаях ее материальный носитель;
2. любая воспринимаемая человеком или машиной информация;
3. информация, зафиксированная на бумажном носителе;
4. информация, зафиксированная на материальном носителе.

Задание № 9
К общедоступной информации можно отнести

1. документы, содержащие персональные данные;
2. конфиденциальную информацию;
3. информацию, доступ к которой ограничен федеральным законом;
4. общеизвестные сведения и иную информацию, доступ к которой не ограничен.

Задание № 10
Безопасность информации включает в себя

1. безопасность информации от внешних воздействий, а также безопасность информации в смысле ее содержания;
2. сведения, подлежащие засекречиванию;
3. сведения, доступ к которым ограничен федеральным законом;
4. конфиденциальность информации.

Задание № 11
Тайну следствия и судопроизводства составляют

1. тайна предварительного расследования и тайна совещания судей;
2. прокурорская и судейская тайны;
3. данные предварительного следствия;
4. служебная тайна.

Задание № 12
К профессиональным тайнам не относится

1. врачебная тайна;
2. адвокатская тайна;
3. тайна частной жизни;
4. тайна исповеди.

Задание № 13
Под преступлениями, посягающими на охраняемую законом информацию, следует понимать

1. предусмотренные уголовным законом общественно опасные деяния, посягающие на общественный порядок и общественную безопасность;
2. предусмотренные уголовным законом общественно опасные деяния, посягающие на информационную безопасность.
3. предусмотренные уголовным законом общественно опасные деяния, посягающие на общественные отношения, складывающиеся по поводу соблюдения установленного порядка обращения с охраняемой законом информацией;
4. предусмотренные уголовным законом общественно опасные деяния, посягающие на безопасность информации.

Задание № 14
Под блокированием компьютерной информации понимается

1. невозможность получить доступ в течение значимого промежутка времени к компьютерной информации ее законному пользователю при сохранности самой информации в памяти компьютера;
2. изменение ее состояния, при котором утрачивается возможность ее восприятия извне кем бы то ни было;
3. любые изменения компьютерной информации, затрудняющие работу законного пользователя;
4. запись оригинальной компьютерной информации на машинный носитель или эвм.

Задание № 15

Какие действия относятся к объективной стороне состава преступления, предусмотренного в ст. 137 УК «Нарушение неприкосновенности частной жизни»

1. незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации;
2. собирание или распространение сведений о частной жизни гражданина, составляющих его личную или семейную тайну, с согласия потерпевшего;
3. нарушение тайны переписки;
4 оглашение сведений о частной жизни гражданина, способствующее повышению его авторитета.

Задание № 16

Преступление, предусмотренное ст. 272 УК «Неправомерный доступ к компьютерной информации», считается оконченным

1. с момента неправомерного доступа к охраняемой законом компьютерной информации;
2. только при наступлении определенных в законе общественно опасных последствий;
3. только при наступлении тяжких последствий;
4. с момента создания угрозы наступления определенных общественно опасных последствий.

Задание № 17

Выберите из приведенных ниже действий те, которые составляют объективную сторону преступления, предусмотренного ст. 275 УК «Государственная измена»

1. шпионаж, совершенный иностранным гражданином;
2. шпионаж, совершенный лицом без гражданства;
3. выдача государственной тайны, совершенная гражданином рф;
4. террористический акт.

Задание № 18

Информационная система это

Ответ:
1. организационно упорядоченная совокупность документов (массивов

документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;
2. организационно упорядоченная совокупность документов(массивов документов);
3. средства вычислительной техники и связи, реализующих информационные процессы;
4. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Задание № 19
Информация о гражданах (персональные данные) это

1. любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу;
2. сведения, которые гражданин не желает распространять;
3. конференциальные сведения о человеке;
4. сведения об обстоятельствах жизни гражданина.

Задание № 20
Какой бывает информация по категории доступа

1. открытая и закрытая;
2. общедоступная и с ограниченным доступом;
3. закрытая и с ограниченным доступом;
4. засекреченная и общедоступная.

Вариант 3

Номер вопроса и проверка сформированной компетенции

№ вопроса	Код компетенции	№ вопроса	Код компетенции	№ вопроса	Код компетенции	№ вопроса	Код компетенции
1	ПК-2 ПК-8	6	ПК-2 ПК-8	11	ПК-2 ПК-8	16	ПК-2 ПК-8
2	ПК-2 ПК-8	7	ПК-2 ПК-8	12	ПК-2 ПК-8	17	ПК-2 ПК-8
3	ПК-2 ПК-8	8	ПК-2 ПК-8	13	ПК-2 ПК-8	18	ПК-2 ПК-8

4	ПК-2 ПК-8	9	ПК-2 ПК-8	14	ПК-2 ПК-8	19	ПК-2 ПК-8
5	ПК-2 ПК-8	10	ПК-2 ПК-8	15	ПК-2 ПК-8	20	ПК-2 ПК-8

Ключ ответов

№ вопроса	верный ответ	№ вопроса	верный ответ	№ вопроса	верный ответ	№ вопроса	верный ответ
1	4	6	1	11	4	16	1
2	4	7	3	12	1	17	2
3	1	8	3	13	1	18	1
4	2	9	3	14	3	19	4
5	3	10	3	15	2	20	1

Задание № 1
НЕ является признаком защищаемой информации

1. защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства;
2. ограничивать доступ к информации может только собственник или уполномоченные на то лица (органа);
3. чем важнее информация, тем тщательнее ее защищают;
4. защищаемая информация не должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства.

Задание № 2
К угрозам информационной безопасности по способу воздействия не относятся

1. информационные;
2. программно-математические;
3. физические угрозы;
4. политические.

Задание № 3
Существующие в современной российской правовой системе тайны можно классифицировать следующим образом

1. государственная тайна и конфиденциальная информация;
2. секретная информация и общедоступная информация;

3. персональные данные и иная секретная информация;
4. конфиденциальная информация и общедоступная информация.

Задание № 4
«Ноу-хау» это

1. информация о поставщиках;
2. информация, составляющая секрет производства;
3. информация о списках работающих;
4. информация о заработной плате.

Задание № 5
В качестве предмета шпионажа выступают

1. сведения, составляющие государственную тайну;
2. любая конфиденциальная информация;
3. сведения, составляющие государственную тайну или иные (не составляющих государственную тайну) сведения для использования их против безопасности рф;
4. сведения, разглашение которых может причинить ущерб РФ.

Задание № 6
Копированием компьютерной информации можно признать действия, связанные с

1. записью оригинальной компьютерной информации на машинный носитель или в средстве вычислительной техники, с условием сохранения формы и содержания такой информации;
2. распечатыванием оригинальной компьютерной информации на средствах вычислительной техники;
3. фотографированием компьютерной информации с монитора;
4. добавление новой компьютерной информации к первоначальной.

Задание № 7
Какое преступление относится к преступлениям в сфере компьютерной информации

1. «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов» (ст. 187 УК РФ);
2. «Незаконные получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну» (ст. 183 УК РФ);
3. «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» (ст. 274 УК РФ);
4. «Нарушение тайны переписки, телефонных переговоров, почтовых,

телеграфных или иных сообщений» (ст. 138 УК РФ).

Задание № 8
При наличии какого условия наступает ответственность по ст. 155 УК «Разглашение тайны усыновления (удочерения)»

1. если эти действия осуществлены без согласия органа опеки и попечительства;
2. если эти действия осуществлены без согласия комиссии по делам несовершеннолетних и защите их прав;
3. если эти действия осуществлены вопреки воле усыновителя;
4. если эти действия осуществлены вопреки воле усыновленного (удочеренного) ребенка.

Задание № 9
Информационная система это

1. отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;
2. любая совокупность информации;
3. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
4. совокупность упорядоченной информации.

Задание № 10
Сведения, составляющие государственную тайну это

1. защищаемые государством сведения в области его военной деятельности, распространение которых может нанести ущерб безопасности рф;
2. любые защищаемые государством сведения;
3. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности рф;
4. защищаемые государством сведения, распространение которых может нанести ущерб безопасности коммерческих организаций.

Задание № 11
Под информационной войной понимаются

1. действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информационным системам противника;
2. действия, направленные на подавление агитационных мероприятий противника;

3. действия, направленные на манипулирование массовым сознанием посредством информации;
4. действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, процессам, основанным на информации, и информационным системам противника при одновременной защите собственной информации.

Задание № 12

По степени секретности сведения, составляющую государственную тайну можно разделить на

1. сведения особой важности, совершенно секретные и секретные;
2. сведения особой важности, совершенно секретные, секретные, конфиденциальные;
3. сведения особой важности, совершенно секретные, секретные, для служебного пользования;
4. сведения совершенно секретные, секретные, закрытая информация.

Задание № 13

Коммерческой тайной не могут являться

1. сведения о численности и составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
2. сведения о структуре управления производством, методика обучения персонала;
3. сведения о маркетинговой политики организации;
4. сведения об источниках финансирования.

Задание № 14

Под компьютерной информацией понимается

1. информация на любом физическом носителе;
2. документированная информация;
3. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи*;*
4. информация в системе средств вычислительной техники.

Задание № 15

Информационно-телекоммуникационная сеть это

1. совокупность двух или более средств вычислительной техники;
2. технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники*;*
3. несколько удаленных друг от друга средств вычислительной техники;
4. несколько взаимосвязанных средств вычислительной техники.

Задание № 16

Субъектом преступлений в сфере компьютерной информации является

1. физическое вменяемое лицо, достигшее 16-летнего возраста;
2. юридические и физические лица, не имеющие разрешения для работы с информацией определенной категории;
3. физическое вменяемое лицо, достигшее 18-летнего возраста;
4. физическое вменяемое лицо, достигшее 14-летнего возраста, имеющее доступ средствам хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационным сетям.

Задание № 17

К тяжким последствиям, как квалифицирующему признаку ст. 273 УК «Создание, использование и распространение вредоносных компьютерных программ», не следует относить

1. утрату конфиденциальной или иной особо ценной информации;
2. заражение компьютерными вирусами нескольких машинных носителей;
3. выход из строя важных технических средств;
4. случаи гибели людей, аварии, катастрофы.

Задание № 18

Субъектом преступления, предусмотренного ст. 189 УК «Незаконные экспорт из Российской Федерации или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники», может быть

1. лицо, наделенное правом осуществлять внешнеэкономическую деятельность;
2. должностное лицо;
3. любое физическое вменяемое и достигшее соответствующего возраста лицо;
4. лицо, имеющее доступ к научно-технической информации.

Задание № 19

К нарушениям правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, влекущим за собой ответственность по ст. 274 УК, не следует относить

1. нарушение правил, содержащихся в общих требованиях по технике

безопасности и эксплуатации компьютерного оборудования;
2. нарушение правил, установленных разработчиками программного обеспечения;
3. нарушение правил, установленных изготовителями компьютерного оборудования;
4. нарушение трудовой дисциплины сетевыми администраторами.

Задание № 20

Свобода поиска, получения, передачи, производства и распространения информации любым законным способом это

1. принцип правового регулирования отношений в сфере информации, информационных технологий и защиты информации;
2. особенности информационно-правовых отношений;
3. обеспечение информационной безопасности.

Вариант 4

Номер вопроса и проверка сформированной компетенции

№ вопроса	Код компетенции	№ вопроса	Код компетенции	№ вопроса	Код компетенции	№ вопроса	Код компетенции
1	ПК-2 ПК-8	6	ПК-2 ПК-8	11	ПК-2 ПК-8	16	ПК-2 ПК-8
2	ПК-2 ПК-8	7	ПК-2 ПК-8	12	ПК-2 ПК-8	17	ПК-2 ПК-8
3	ПК-2 ПК-8	8	ПК-2 ПК-8	13	ПК-2 ПК-8	18	ПК-2 ПК-8
4	ПК-2 ПК-8	9	ПК-2 ПК-8	14	ПК-2 ПК-8	19	ПК-2 ПК-8
5	ПК-2 ПК-8	10	ПК-2 ПК-8	15	ПК-2 ПК-8	20	ПК-2 ПК-8

Ключ ответов

№ вопроса	верный ответ	№ вопроса	верный ответ	№ вопроса	верный ответ	№ вопроса	верный ответ
1	2	6	2	11	1	16	2
2	2	7	2	12	1	17	4
3	3	8	2	13	4	18	4

4	2	9	1	14	2	19	1
5	1	10	1, 3, 4	15	1	20	3

Задание № 1

Основной объем прав на информацию содержится в следующей норме Конституции Российской Федерации:

1. «каждому гарантируется право свободно получать, производить и распространять информацию…»;
2. «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом...»;
3. «каждый имеет право на свободу получения и передачи информации в любом виде…».

Задание № 2

Доктрина информационной безопасности Российской Федерации содержит в себе:

1. три составляющих национальных интересов России;
2. четыре составляющих национальных интересов России;
3. пять составляющих национальных интересов России.

Задание № 3

Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него, — это:

1. специальные реквизиты;
2. условия специального допуска;
3. гриф секретности.

Задание № 4

Сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность:

1. банк данных на граждан;
2. информация о гражданах (персональные данные);
3. сведения о гражданах, их личной жизни.

Задание № 5

Надзор в информационной сфере, в пределах компетенции, осуществляет:

1. прокуратура;

2. органы исполнительной власти субъектов федерации;
3. совет по информационному обществу.

Задание № 6
Объективная сторона информационной безопасности - это:

1. психологическое отношение граждан к вопросу правового регулирования отношений в сфере информационной безопасности;
2. система норм права об информационной безопасности;
3. система охранительных действий субъектов информационного права в отношении объекта охраны.

Задание № 7
К числу прав субъекта персональных данных относится:

1. право на выбор вида обработки персональных данных автоматизированная, неавтоматизированная);
2. право на доступ к своим персональным данным;
3. право контролировать деятельность оператора персональных данных.

Задание № 8
К служебной тайне не относится ...

1. тайна деятельности соответствующего органа
2. вред, причиненный здоровью работника в связи с производственной травмой
3. профессиональная тайна

Задание № 9
Режим защиты информации не устанавливается в отношении сведений, относящихся к ...

1. деятельности государственных деятелей
2. персональным данным
3. государственной тайне
4. конфиденциальной информации

Задание № 10
Доступ к сведениям, составляющим налоговую тайну, имеют должностные лица в соответствии с перечнями, определяемыми:

1. Министерством внутренних дел РФ
2. Правительством РФ
3. Федеральной налоговой службой
4. Федеральной таможенной службой

Задание № 11
Информационные ресурсы подразделяются на открытую информацию и информацию с ограниченным доступом по:

1. режиму доступа
2. виду собственника
3. виду носителя
4. способу формирования и распространения информации

Задание № 12
Правовое регулирование служебной тайны в российском законодательстве основывается на нормах

1. Гражданского кодекса РФ
2. Специальных нормативных правовых актах о служебной тайне
3. Кодекса РФ об административных правонарушениях
4. Трудового кодекса РФ

Задание № 13
Признак, не относящийся к коммерческой тайне

1. информация имеет действительную или потенциальную коммерческую ценность
2. обладатель информации принимает меры к охране ее конфиденциальности
3. отсутствует свободный доступ к информации
4. сведения, содержащие коммерческую тайну, устанавливаются учредительными документами

Задание № 14
Согласно легальному определению информация - это

1. сведения о каких-либо событиях, явлениях, процессах, передаваемые от человека к человеку
2. сведения (сообщения, данные) независимо от формы их представления
3. сообщение, переданное или полученное пользователем информационно - телекоммуникационной сети.

Задание № 15
Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства

1. угроза информационной безопасности;

2. предполагаемые действия иностранных государств;
3. деятельность иностранных разведок.

Задание № 16
К действиям по неправомерному доступу к охраняемой законом компьютерной информации относятся

1. похищение компьютера;
2. всякая форма проникновения к ней с использованием средств (вещественных и интеллектуальных) электронно-вычислительной техники, позволяющая манипулировать информацией (уничтожать ее, блокировать, модифицировать, копировать);
3. завладение любым машинным носителем информации как вещью;
4. уничтожение, блокирование, модификация либо копирование информации.

Задание № 17
К угрозам информационной безопасности по способу воздействия не относятся

1. информационные;
2. программно-математические;
3. физические угрозы;
4. политические.

Задание № 18
Под информационной войной понимаются

1. действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информационным системам противника;
2. действия, направленные на подавление агитационных мероприятий противника;
3. действия, направленные на манипулирование массовым сознанием посредством информации;
4. действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, процессам, основанным на информации, и информационным системам противника при одновременной защите собственной информации.

Задание № 19
Субъектом преступлений в сфере компьютерной информации является

1. физическое вменяемое лицо, достигшее 16-летнего возраста;

2. юридические и физические лица, не имеющие разрешения для работы с информацией определенной категории;
3. физическое вменяемое лицо, достигшее 18-летнего возраста;
4. физическое вменяемое лицо, достигшее 14-летнего возраста, имеющее доступ средствам хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационным сетям.

Задание № 20
Понятие «информационная безопасность» закреплено

1. в Законе Российской Федерации от 27 декабря 1991 г. №1224-11 «О средствах массовой информации»;
2. в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. в Доктрине информационной безопасности Российской Федерации.