

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра информационного права и информатики

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

Правовые основы информационной безопасности

Образовательная программа
40.03.01 Юриспруденция
Профили подготовки
государственно-правовой
гражданско-правовой
уголовно-правовой

Форма обучения: **очная, - , заочная**

Статус дисциплины: **входит в обязательную часть ОПОП**

Махачкала
2021 год

Фонд оценочных средств по дисциплине «Правовые основы информационной безопасности» составлен в 2021 году в соответствии с требованиями ФГОС ВО-бакалавриат по направлению подготовки 40.03.01 Юриспруденция от «13» августа 2020 г. №1011.

Разработчик(и): кафедра «Информационное право и информатика»,
Рагимханова Камилла Тагировна, старший преподаватель.

Фонд оценочных средств одобрен:
на заседании кафедры информационного права и информатики
от «11» 05 2024 г., протокол №10
Зав. кафедрой Абдусаламов Р.А.

на заседании Методической комиссии юридического института
от «29» 06 2024 г., протокол №10.
Председатель Арсланбекова А.З.

Фонд оценочных средств согласован с учебно-методическим управлением
Начальник УМУ Гасангаджиева А.Г.
«09» 07 2024 г.

Рецензент:

преп-м каф. ИСиП
(полное наименование организации
и должности руководителя)

Ия
(подпись) / Муталишова З.Р.
(Фамилия И.О.)

ПАСПОРТ
Фонда оценочных средств

по дисциплине «Правовые основы информационной безопасности»

1.1. Основные сведения о дисциплине

Общая трудоемкость дисциплины составляет 2 зачетных единиц (72 академических часа).

Очная форма обучения

Вид работы	2 семестр	Всего
Общая трудоёмкость	72	72
Контактная работа:	24	24
Лекции(Л)	12	12
Практические занятия (ЛЗ)	12	12
Консультации		
KCP		
Контроль		
Промежуточная аттестация(зачет,	Зачет	
Самостоятельная работа:	48	48
• написание эссе (<i>реферат</i>);	12	12
• самоподготовка (<i>проработка и повторение лекционного материала и материала учебников и учебных пособий</i>);	10	10
• решение тестовых заданий;	10	10
• решение задач и т.п.	14	14

Заочная форма обучения

Вид работы	2 семестр	Всего
Общая трудоёмкость	72	72
Контактная работа:	8	8
Лекции(Л)	6	6
Практические занятия (ЛЗ)	2	2
Консультации		
KCP		
Контроль		
Промежуточная аттестация(зачет)	Зачет	
Самостоятельная работа:	64	64
• написание эссе (<i>реферата</i>);	16	16
• самоподготовка (<i>проработка и повторение лекционного материала и материала учебников и учебных пособий</i>);	16	16
• решение тестовых заданий;	10	16

Очно- форма обучения

Вид работы	2 семестр	Всего
Общая трудоёмкость	72	72
Контактная работа:	24	24
Лекции(Л)	10	10
Практические занятия (ЛЗ)	10	10
Консультации		
KCP		
Контроль		
Промежуточная аттестация(зачет,	Зачет	
Самостоятельная работа:	52	52
• написание эссе (<i>реферат</i>);	12	12
• самоподготовка (<i>проработка и повторение лекционного материала и материала учебников и учебных пособий</i>);	12	12
• <i>решение тестовых заданий</i> ;	10	10
• <i>решение задач и т.п.</i>	14	14

1.2. Требования к результатам обучения по дисциплине, формы их контроля и виды оценочных средств

№ п/п	Контролируемые модули,разделы (темы) дисциплины	Индекс контролируемых компетенций(илиеёчастей)	Оценочные средства		Способ контроля
			наименование	№ заданий	
1	Основные понятия курса «правовые основы информационной безопасности»	УК-1 ОПК-8 ОПК-9	Контрольные вопросы Эссе (реферат) Тесты	В соответствии с темой 1-3 Тема 1	Устно, письменно, Устно Компьютерное тестирование
2	Информационная безопасность системе национальной безопасности РФ	УК-1 ОПК-8 ОПК-9	Контрольные вопросы Эссе (реферат) Тесты	В соответствии с темой 3-9 Тема 2	Устно, письменно, Устно Компьютерное тестирование
3	Правовые основы обеспечения информационной безопасности	УК-1 ОПК-8 ОПК-9	Контрольные вопросы Эссе (реферат) Решение задач Тесты	В соответствии с темой 10-12 №1 Тема 3	Устно Устно Письменно Компьютерное тестирование
4	Организационное обеспечение информационной безопасности	УК-1 ОПК-8 ОПК-9	Контрольные вопросы Эссе (реферат) Решение задач Тесты	В соответствии с темой 13-15 №2 Тема 4	Устно Устно Письменно Компьютерное тестирование

5	Правовые режимы конфиденциальной информации	УК-1 ОПК-8 ОПК-9	Контрольные вопросы Эссе (реферат) Решение задач Тесты	В соответствии с темой 16-18 №3 Тема 5	Устно Устно Письменно Компьютерное тестирование
6	Ответственность правонарушения информационной сфере	УК-1 ОПК-8 ОПК-9	Контрольные вопросы Эссе (реферат) Решение задач Тесты	В соответствии с темой 19-20 №4 Тема 6	Устно Устно Письменно Компьютерное тестирование

1.3. Показатели и критерии определения уровня сформированности компетенций

№ п/ п	Индекс компетен- ции	Уровни сформированности компетенции			
		Недостаточный	Удовлетворитель- ный (достаточный)	Базовый	Повышенный
1	УК-1	Отсутствие признаков удовлетворительного уровня	Знает: принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач Умеет: анализировать и систематизировать данные, оценивать эффективность процедур анализа проблем и принятия решений в профессионально	Знает: систему учета и принципы калькулирования и систематизации, системообразующие элементы принципы их формирования Умеет: анализировать, толковать и правильно применять правовые нормы; осуществлять комплексный	Знает: правильно и логично рассуждать, отличать факты от мнений. Умеет: Определять и оценивать практические последствия возможных решений задачи. Владеет: навыками логично и аргументировано рассуждать.

			й деятельности Владеет: навыками научного поиска и практической работы с информационными источниками; методами принятия решений	сравнительно-правовой анализ нормативных актов Владеет: основными навыками правового анализа; навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности	
2	ОПК-8	Отсутствие признаков довлетворител ьного уровня	Знает: основные правовые базы данных, принципы их работы Умеет: пользоваться компьютером как средством управления и обработки информационных массивов, работать с информацией в глобальных компьютерных сетях Владеет: приемами и навыками использования компьютера как	Знает: основы информатики и информационных технологий, приемы и способы обработки и систематизации информации Умеет: использовать правовые базы данных при решении задач профессиональной деятельности, соблюдая требования информационной	Знает: решение конкретных задач профессиональной деятельности с учетом требований информационной безопасности Умеет: извлекать из различных источников, включая правовые базы данных, юридически значимую

		средства управления и обработки информационных массивов, работы с информацией в глобальных компьютерных сетях при осуществлении профессиональной деятельности.	безопасности Владеет: необходимыми знаниями и навыками для решения задач профессиональной деятельности с учетом требований информационной безопасности	информацию, обрабатывает и систематизирует ее в соответствии с поставленной целью Владеет: информационными технологиями для решения конкретных задач профессиональной деятельности с учетом требований информационной безопасности
3	ОПК-9	Отсутствие признаков удовлетворительного уровня	Знает: основные современные информационные технологии, используемые в практической юридической деятельности; Умеет: работать с информационными системами и сервисами, используемыми в практической юридической деятельности государственным и органами, в том числе правоохранительными органами, органами	Знает: принципы работы современных информационных технологий, используемых в практической юридической деятельности Умеет: определять необходимые в профессиональной деятельности цифровые инструменты для решения конкретной профессиональной задачи Владеет: навыками

		<p>местного самоуправления, организациями.</p> <p>Владеет: навыками работы с информационными системами и сервисами, используемыми в практической юридической деятельности по месту прохождения практической подготовки</p>	<p>Владеет: навыками организации профессиональной деятельности в онлайнформате с использованием цифровых сервисов.</p>	<p>получения, создания и использования информационных продуктов в профессиональной сфере</p>
--	--	--	--	--

2. КОНТРОЛЬНЫЕ ЗАДАНИЯ И ИНЫЕ МАТЕРИАЛЫ ОЦЕНКИ знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения дисциплины «Правовые основы информационной безопасности»

Контрольные вопросы по темам

Тема 1. Основные понятия курса «Правовые основы информационной безопасности»

1. Особенности информации как объекта правового регулирования.
2. Какие отношения составляют предмет правовых основ информационной безопасности?
3. Какова система правового обеспечения информационной безопасности?

Тема 2. Информационная безопасность системе национальной безопасности РФ

1. Какую роль играет национальная безопасность в информационной безопасности?
2. Назовите федеральные законы, регулирующие информационную безопасность.
3. Какие нормативные акты Республики Дагестан регулируют информационную безопасность в системе национальной безопасности?

Тема 3. Правовые основы обеспечения информационной безопасности

1. Дайте понятие правовых основ обеспечения информационной безопасности.
2. Назовите понятия, закрепленные в Доктрине информационной безопасности.
3. Раскройте угрозы информационной безопасности.

Тема 4. Организационное обеспечение информационной безопасности

1. Дайте понятие организационного обеспечения информационной безопасности.
2. Какие вы знаете случаи нарушения организационного обеспечения информационной безопасности?
3. Какие вы знаете основания для установления криптографических методов защиты информации?

Тема 5. Правовые режимы конфиденциальной информации

1. Назовите понятие, признаки и содержания правового режима информации.
2. Раскройте элементы правового режима информации.
3. Перечислите сходства и различия тайны и конфиденциальности.

Тема 6. Ответственность правонарушения информационной сфере

1. Перечислите понятие и признаки преступлений (правонарушений) в информационной сфере.
2. Раскройте понятие и содержание ответственности в информационной сфере.
3. Раскройте виды ответственности в информационной сфере.

Критерии оценки:

-оценка «отлично» выставляется студенту, если даны исчерпывающие и обоснованные ответы на все поставленные вопросы, при ответах выделялось главное, развернутый ответ без принципиальных ошибок; логически выстроенное содержание ответа; мысли излагались в логической последовательности; показано умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии; полное знание терминологии по данной теме

-оценка «хорошо» выставляется студенту, если Даны полные, достаточно обоснованные ответы на поставленные вопросы, при ответах не всегда выделялось главное, в основном были краткими, но не всегда четкими; практически полное знание терминологии данной темы

- оценка «удовлетворительно» выставляется студенту, если даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования, при решении практических задач студент использовал прежний опыт и не

применил новые знания, однако, на уточняющие вопросы даны правильные ответы; при ответах не выделялось главное; ответы были многословными, нечеткими и без должной логической последовательности; на отдельные дополнительные вопросы не даны положительные ответы

-оценка «неудовлетворительно» - выставляется студенту при неполном и некорректном ответе

Кейс-задачи

Кейс-задача №1

1. Духонин К.В. находясь в студии радио «Эхо Москвы» в Перми и участвуя в прямом эфире радиопередачи в ходе разговора о проблемах в сфере образования, не имея подтверждающих фактов, сообщил заведомо ложные сведения о гр. Шулькине И.Г., занимающем должность заместителя главы администрации г. Перми, являющимся должностным лицом, которые порочат честь и достоинство и подрывают репутацию последнего.

Духонин К.В. может быть привлечен к ... ответственности.

1. уголовной
2. административной
3. гражданской

2. Духонин К.В. находясь в студии радио «Эхо Москвы» в Перми и участвуя в прямом эфире радиопередачи в ходе разговора о проблемах в сфере образования, не имея подтверждающих фактов, сообщил заведомо ложные сведения о гр. Шулькине И.Г., занимающем должность заместителя главы администрации г. Перми, являющимся должностным лицом, которые порочат честь и достоинство и подрывают репутацию последнего.

За этот вид правонарушения предусматривают ответственность нормы таких нормативно-правовых актов, как ...

1. УК РФ ст. 128.1
 2. Закон РФ "О СМИ", ст. 57 **Освобождение от ответственности**
 3. ФЗ «Об информации, информационных технологиях и о защите информации», ст.2
 4. Закон РФ "О СМИ", ст. 47 Права журналистов
3. Духонин К.В. находясь в студии радио «Эхо Москвы» в Перми и участвуя в прямом эфире радиопередачи в ходе разговора о проблемах в сфере образования, не имея подтверждающих фактов, сообщил заведомо ложные сведения о гр. Шулькине И.Г., занимающем должность заместителя главы администрации г. Перми, являющимся должностным лицом, которые порочат честь и достоинство и подрывают репутацию последнего.

Для виновника данного правонарушения может быть предусмотрен такой вид наказания, как ...

Кейс-задача №2

1. В районной газете была опубликована статья о проблеме социальной беспризорности, когда дети, при живых родителях, не обеспечивающих им должного ухода и воспитания, по сути становятся беспризорными, вынуждены побираться в поисках куска хлеба, живут в неподобающих условиях. Материал был подготовлен на примере одной семьи. Орган опеки и

попечительства района пригласил журналиста газеты в рейд направленный на отобрание детей у матери, ведущей беспорядочный образ жизни. Журналист посетила семью вместе с сотрудниками отдела опеки и попечительства, при их участии беседовала с детьми, сделала фотографию детей перед их посадкой в машину, принадлежащую отделу опеки и попечительства. Публикация была посвящена общественно-значимой теме, обращалась к жителям района, поднимала проблему недостаточного внимания общества к нуждам детей, проживающих в неблагополучных семьях.

Установите соответствие между понятиями и их формулировкой.

1. персональные данные
2. распространение персональных данных
3. предоставление персональных данных
4. обезличивание персональных данных
 - a) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
 - b) действия, направленные на раскрытие персональных данных неопределенному кругу лиц
 - c) действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
 - d) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
2. В районной газете была опубликована статья о проблеме социальной беспризорности, когда дети, при живых родителях, не обеспечивающих им должного ухода и воспитания, по сути становятся беспризорными, вынуждены побираться в поисках куска хлеба, живут в неподобающих условиях. Материал был подготовлен на примере одной семьи. Орган опеки и попечительства района пригласил журналиста газеты в рейд направленный на отобрание детей у матери, ведущей беспорядочный образ жизни. Журналист посетила семью вместе с сотрудниками отдела опеки и попечительства, при их участии беседовала с детьми, сделала фотографию детей перед их посадкой в машину, принадлежащую отделу опеки и попечительства. Публикация была посвящена общественно-значимой теме, обращалась к жителям района, поднимала проблему недостаточного внимания общества к нуждам детей, проживающих в неблагополучных семьях.

Журналист имеет право размещать персональные данные несовершеннолетних с согласия ...

- 1) их законных представителей
 - 2) детей
 - 3) органов опеки
 - 4) родителей
3. В районной газете была опубликована статья о проблеме социальной беспризорности, когда дети, при живых родителях, не обеспечивающих им должного ухода и воспитания, по сути становятся беспризорными, вынуждены побираться в поисках куска хлеба, живут в неподобающих

условиях. Материал был подготовлен на примере одной семьи. Орган опеки и попечительства района пригласил журналиста газеты в рейд направленный на отобрание детей у матери, ведущей беспорядочный образ жизни. Журналист посетила семью вместе с сотрудниками отдела опеки и попечительства, при их участии беседовала с детьми, сделала фотографию детей перед их посадкой в машину, принадлежащую отделу опеки и попечительства. Публикация была посвящена общественно-значимой теме, обращалась к жителям района, поднимала проблему недостаточного внимания общества к нуждам детей, проживающих в неблагополучных семьях.

Журналист за разглашение персональных данных несовершеннолетних может быть привлечен к такому виду ответственности, как ...

Кейс-задача №3

1. Информация впервые введена в состав Гражданского кодекса РФ как вид объекта гражданских прав. Информация активно используется в системах гражданского и публичного права не только как объект самостоятельного оборота, но и как доказательственное средство в отношениях между субъектами.

При передаче информации от одного субъекта к другому процедура отчуждения носителя с информацией должна сопровождаться

- 1) передачей прав на ее использование
- 2) физическим удалением информации со всех носителей прежнего обладателя
- 3) передачей права автора на нее

2. Информация впервые введена в состав Гражданского кодекса РФ как вид объекта гражданских прав. Информация активно используется в системах гражданского и публичного права не только как объект самостоятельного оборота, но и как доказательственное средство в отношениях между субъектами.

Установите соответствие между признаками информации и ее юридическими свойствами

- | | |
|--|---|
| 1. Идеальность и субстанциональная несамостоятельности информации | а) двуединство информации и материального носителя, на котором она закрепляется |
| 2. Неисчерпаемость информации | б) бесконечный неисчерпаемый ресурс, ее физическая неотчуждаемость от создателя, обладателя и потребителя |
| 3. Качественные характеристики | с) субъективная ценность информации и нелинейность |
| 3. Информация впервые введена в состав Гражданского кодекса РФ как вид объекта гражданских прав. Информация активно используется в системах гражданского и публичного права не только как объект самостоятельного оборота, но и как доказательственное средство в отношениях между | |

субъектами. В информационном праве информацию следует определять, как основной ...

Кейс-задача №4

1. Программист Алиев А.Д. был принят на работу в компанию «Гамма Плюс», где на него возлагались функции оператора ПК по вводу законодательства в информационные базы, которые «Гамма Плюс» продавала на коммерческой основе предприятиям легкой промышленности. В свободное от ввода информации время Алиеву удалось разработать и внедрить более совершенный алгоритм обработки правовой информации в информационной базе, что заметно повысило ее ценность и привело к получению значительной прибыли.

Алиев потребовал от руководства компании «Гамма Плюс» отчисления всей прибыли за реализацию модернизированной им программы. Квалифицируйте его требования.

- 1) Он не вправе требовать, так как он не является автором всей информационной базы
- 2) Он не вправе требовать, так как ему выплачивается заработка плата
- 3) Он вправе требовать, так как его изменения привели к увеличению прибыли
- 4) Он не вправе требовать, так как он является автором всей информационной базы

2. Программист Алиев А.Д. был принят на работу в компанию «Гамма Плюс», где на него возлагались функции оператора ПК по вводу законодательства в информационные базы, которые «Гамма Плюс» продавала на коммерческой основе предприятиям легкой промышленности. В свободное от ввода информации время Алиеву удалось разработать и внедрить более совершенный алгоритм обработки правовой информации в информационной базе, что заметно повысило ее ценность и привело к получению значительной прибыли.

Возникшие между Алиевым и компанией «Гамма Плюс» отношения в связи с этой разработкой будут регулироваться ... частью Гражданского кодекса.

3. Программист Алиев А.Д. был принят на работу в компанию «Гамма Плюс», где на него возлагались функции оператора ПК по вводу законодательства в информационные базы, которые «Гамма Плюс» продавала на коммерческой основе предприятиям легкой промышленности. В свободное от ввода информации время Алиеву удалось разработать и внедрить более совершенный алгоритм обработки правовой информации в информационной базе, что заметно повысило ее ценность и привело к получению значительной прибыли.

Установите соответствие между объектами авторских и патентных прав

1. Объект авторского права
2. Объект патентного права
 - a) производные произведения, то есть произведения, представляющие собой переработку другого произведения

b) результаты интеллектуальной деятельности в сфере дизайна

Критерии оценки

- ***оценка «отлично»*** выставляется студенту, если он правильно ответил на все вопросы по задаче и обосновал свои ответы ссылками на источники права.
- ***оценка «хорошо»*** выставляется студенту, если он правильно ответил на все вопросы по задаче.
- ***оценка «удовлетворительно»*** выставляется студенту, если он знает, к какой теме относится казус, способен проанализировать фабулу задачи, сформулировать вопросы, ответы на которые способствуют решению задачи в целом.
- ***оценка «неудовлетворительно»*** – задача решена неправильно

Комплект тестов (тестовых заданий)

Тема 1. Основные понятия курса «Правовые основы информационной безопасности»

1. В ст.2 ФЗ «Об информации, информационных технологиях и о защите информации» информация определена как
 - 1) сведения (сообщения, данные) независимо от формы их представления
 - 2) универсальная субстанция, пронизывающая все сферы человеческой деятельности, служащая проводником знаний и сведений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения
 - 3) основной объект, по поводу которого или в связи, с которым возникают общественные отношения, подлежащие регулированию правом
2. Основные признаки информации, имеющие универсальный характер и проявляющиеся в любых формах ее существования
 - 1) все верны
 - 2) идеальность и субстанциональная несамостоятельность; неисчерпаемость; преемственность; селективность; трансформируемость; универсальность; комплексное качество
 - 3) адекватность; достоверность; полнота; избыточность; доступность; ценность
3. Информационная сфера (среда) – это
 - 1) сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации
 - 2) сфера деятельности, связанная с правовым регулированием информационных отношений, возникающих в обществе
 - 3) процесс сбора, обработки, накопления, хранения, поиска, получения, распространения и потребления информации

4. Информационная сфера как сфера правового регулирования представляет собой

1) совокупность субъектов права, объектов права, социальных отношений, регулируемых правом или подлежащих правовому регулированию

2) процесс сбора, обработки, накопления, хранения, поиска, получения, распространения и потребления информации

3) социальные (общественные) отношения, возникающие при выполнении информационных процессов и подлежащих правовому регулированию

5. Под объектами информационных правоотношений понимают) блага, существующие в формах информации, документированной информации и информационных систем, по поводу которых возникает и осуществляется деятельность участников этих правоотношений

1) блага, возникающие при осуществлении поиска, получения и потребления информации, информационных ресурсов, информационных продуктов, информационных услуг

2) блага, возникающие при создании и применении информационных систем, их сетей, средств обеспечения;

3) блага, возникающие при создании средств и механизмов информационной безопасности

6. Дайте определение информационной сферы_____

7. Основными областями информационной сферы являются_____

8. Основные признаки информации, имеющие универсальный характер и проявляющиеся в любых формах ее существования (несколько правильных ответов)

1) идеальность и субстанциональная несамостоятельность;

2) неисчерпаемость

3) системность

9. Установите соответствие между признаком информации и его утверждением

1.Неисчерпаемость информации

2. Преемственность информации

3. Селективность информации

а) информация при ее передаче может иметь неограниченное число пользователей и при этом оставаться неизменной

б) проявляется в том, что всем изменениям информации сопутствуют изменения в материальных системах, носящие поступательный характер

в) означает возможность выбора или отбора информации при ее использовании, накоплении или переработки.

Тема 2. Информационная безопасность в системе национальной безопасности РФ

1. В законе РФ «О безопасности» безопасность определяется как

1) как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз

2) совокупность потребностей, удовлетворение которых обеспечивает существование и возможности прогрессивного развития личности, общества, государства

3) проведение единой государственной политики в этой сфере и система мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства, направленных на выявление и предупреждение угроз

2. По определению, данному Г.В. Емельяновым и А.А. Стрельцовым, под информационной войной понимается

1) «особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств»

2) совокупность запланированных, взаимосвязанных информационных операций, успешное выполнение которых приводит к достижению цели, как правило, заключающейся во взятии под контроль системы управления противника (государства) или слому этой системы управления и замены ее на другую — контролируемую

3) «специальные средства, технологии и информацию, позволяющие осуществлять «силовое» воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, экономическим и другим жизненно важным интересам государства»

3. С.П. Растиоргуев определяет понятие «информационное оружие»

1) как «открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере»

2) как «специальные средства, технологии и информацию, позволяющие осуществлять «силовое» воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, экономическим и другим жизненно важным интересам государства»

3) как совокупность запланированных, взаимосвязанных информационных операций, успешное выполнение которых приводит к достижению цели, как правило, заключающейся во взятии под контроль системы управления противника (государства) или слому этой системы управления и замены ее на другую — контролируемую

4. К правовым методам, обеспечивающим информационную безопасность, относятся:

1) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Разработка аппаратных средств обеспечения правовых данных

3) Разработка и установка во всех компьютерных правовых сетях журналов учета действий

5. К основным принципам обеспечения информационной безопасности относится:

- 1) Экономической эффективности системы безопасности
- 2) Многоплатформенной реализации системы
- 3) Усиления защищенности всех звеньев системы

6. В Концепции национальной безопасности РФ определены интересы государства (несколько вариантов)

- 1)которые состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России,
- 2)в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии международного сотрудничества
- 3)установлены в упрочении демократии, создании правового государства, достижении и поддержании общественного согласия, духовном обновлении России
- 4)как полное обеспечение конституционных прав и свобод, личной безопасности, повышение качества и уровня жизни, физическое, духовное и интеллектуальное развитие

7. Установите соответствие между автором определения «информационного оружия» и его утверждением

1. Г.В. Емельянов и А.А. Стрельцов

2. С.П. Расторгуев

a) Информационное оружие - это «специальные средства, технологии и информацию, позволяющие осуществлять «силовое» воздействие на информационное пространство общества и привести к значительному ущербу политическим, оборонным, экономическим и другим жизненно важным интересам государства»

b) Информационное оружие - это «открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере»

8. Расположите в хронологическом порядке следующие информационные войны

- a) «Бархатные» революции в странах Восточной Европы
- b) Августовский путч в СССР
- c) Агрессия в Югославии
- d) «Революция роз» в Грузии
- e) «Оранжевая революция» в Украине
- f) Гуманитарная катастрофа в Южной Осетии

9. Установите соответствие между определением и его утверждением

1. история оружия в гуманитарной сфере
2. история оружия в технической сфере

a) это история СМИ и технологий скрытного управления человеком (гипноз, реклама, специальные учения, НЛП-программирование и т.п.)

б) это история программных средств скрытого информационного воздействия (вирусы, закладки) и информационных технологий их применения

Тема 3. Правовые основы обеспечения информационной безопасности

1. Структура информационного законодательства включает

1) информационно-правовые нормы международного законодательства; информационно-правовые нормы Конституции РФ; нормативно-правовые акты отрасли информационного законодательства

2) международные акты информационного законодательства; информационно-правовые нормы Конституции РФ; отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства

3) информационно-правовые нормы Конституции РФ; отрасли законодательства, акты которых целиком посвящены вопросам информационного законодательства; отрасли законодательства, акты которых включают отдельные информационно-правовые нормы информационных ресурсов и предоставлении информации из них пользователю

2. Акты отрасли информационного законодательства условно подразделяются

1) акты, «образующие» систему информационного законодательства как единый, цельный механизм правового регулирования отношений в информационной сфере, и акты, регулирующие отдельные направления в соответствии с установленными в общей части принципами, нормами и правилами

2) отраслевые, межотраслевые и смежные

3) императивные и диспозитивные

3. Под объектами информационных правоотношений понимают

1) блага, существующие в формах информации, документированной информации и информационных систем, по поводу которых возникает и осуществляется деятельность участников этих правоотношений

2) блага, возникающие при осуществлении поиска, получения и потребления информации, информационных ресурсов, информационных продуктов, информационных услуг

3) блага, возникающие при создании и применении информационных систем, их сетей, средств обеспечения;

4. Основными направлениями правового регулирования отношений в Интернет являются

1) защита от вредной и незаконной информации; соблюдение авторских и смежных прав; вопросы электронного документооборота; вопросы киберэкономики; информационная безопасность; правонарушения

2) информационная безопасность; вопросы разработки сетевых программ и техники; повышение производительности каналов сети; вопросы электронного документооборота; вопросы киберэкономики; правонарушения

3) использование электронной подписи и электронных денег; ограничение права доступа к информации; охрана прав несовершеннолетних

5. При правовом регулировании отношений в Интернет важно соблюдение баланса

1) между свободой слова и интересами несовершеннолетних; свободы доступа к информации и информационной безопасностью; свободы производства информации и ограничения производства и распространения опасной информации

2) между свободой слова и интересами несовершеннолетних; между свободой слова и цензурой; свободы к государственным ресурсам и их безопасностью

3) свободы производства информации и ограничения производства и распространения опасной информации; между использованием различных видов каналов (кабельных, спутниковых, радиопоисковых и т.п.); между программными и техническими средствами защиты информации

6. Расположите в хронологическом порядке принятия следующих федеральных законов РФ

1. «Об информации, информационных технологиях и о защите информации»
2. «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»,
3. «О защите детей от информации, причиняющей вред их здоровью и развитию»,
4. «Об электронной подписи»

Тема 4. Правовые режимы конфиденциальной информации

1. Правовой режим информации - это

1) объектный режим, вводимый законодательным актом и позволяющий обеспечить комплексность воздействия в информационной сфере посредством совокупности регулятивных, охранительных, процессуально-процедурных средств, характеризующих особое сочетание дозволений, запретов и обязываний, а также гарантий по его соблюдению

2) порядок регулирования, выраженный в комплексе правовых средств, которые характеризуют особое сочетание взаимодействующих между собой дозволений, запретов, а также позитивных обязываний и создают особую направленность регулирования

3) государственный строй, совокупность средств, методов, способов осуществления власти

2. Правовой режим объекта правоотношения может быть

1) общим (или первичным) и специальным (или вторичным)

2) императивным и диспозитивным

3) открытым и ограниченным

3. Специальный (или вторичный) правовой режим – это режим

1) вносящий либо особые льготы и преимущества, либо особые ограничения, которые заключаются в дополнительных запретах и обязываниях

- 2) при котором участники отношений не могут изменить по своему усмотрению установленные правила поведения
- 3) при котором участники отношений могут менять по своему усмотрению правила поведения
4. Правовой режим информации определяется нормами, устанавливающими:
- 1) порядок документирования информации; право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах; категорию информации по уровню доступа к ней; порядок правовой защиты информации
 - 2) порядок производства, передачи и распространения информации
 - 3) порядок создания и применения информации, информационных систем и механизмов информационной безопасности
5. К публично-правовым отношениям относятся (несколько правильных ответов):
- 1) отношения, возникающие при создании и функционировании "электронного правительства"
 - 2) отношения по лицензированию деятельности провайдеров, удостоверяющих центров и иных субъектов, по регистрации электронных СМИ и сертификации технических средств; отношения по привлечению к ответственности за преступления и правонарушения, совершенные с использованием Интернета
 - 3) в сфере электронной коммерции - отношения типа B2A – Business to Administration
7. Отличие тайны от конфиденциальности _____
8. Документирование информации- это_____
9. Установите соответствие между элементами правового режима информации и его утверждением
1. Целевое назначение
 2. Объект правового регулирования
 3. Правовое положение субъектов правового режима
 4. Комплекс способов правового регулирования и средств юридического воздействия
 - a) заключающееся в установлении прав и обязанностей субъектов по поводу информации, их защите, обеспечении информационной безопасности и баланса интересов личности, общества, государства
 - b) информация, обладающая общими свойствами, характерными для любых видов информации
 - c) характеризуемое с точки зрения их равенства: равное и неравное.
 - d) включающий основные способы правового регулирования (дозволение, запрещение, позитивное обязывание), направленные на поддержание режима в заданных параметрах и выражены в юридических нормах.

Тема 5. Организационное обеспечение информационной безопасности

1. Кто является основным ответственным за определение уровня классификации информации?

- 1) владелец
- 2) Высшее руководство
- 3) руководитель организации

2. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

- 1)руководство
- 2) владельцы
- 3)пользователи

3. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

- 1) поддержка высшего руководства
- 2) эффективные и защитные методы
- 3) актуальные и адекватные политики безопасности

4. Политика безопасности-это:

- 1)широкие, высокоуровневые заявления руководства
- 2)пошаговые инструкции по выполнению задач безопасности
- 3)детализированные документы по обработке инцидентов безопасности

5. Эффективная программа безопасности требует сбалансированного применения:

- 1)технических и нетехнических методов
- 2)физической безопасности
- 3)процедур безопасности и шифрования

6. Согласно ст.16 ч.1 ФЗ «Об информации, информационных технологиях и о защите информации» защита информации представляет собой (множественный выбор)

- a) - принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерных действий
- b) - соблюдение конфиденциальности информации ограниченного доступа, реализацию права на доступ к информации
- c) - защиту интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации
- d) - защиту информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц

7. Установите соответствие между формулировкой направлений защиты и их содержанием

- 1) защита интересов личности, общества, государства от угроз воздействия недоброкачественной информации, от нарушения порядка распространения информации
- 2) защита прав и свобод в информационной сфере в условиях информатизации

- 3) защита информации, информационных ресурсов и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц
- a) чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности; нравственных и эстетических идеалов; стабильности и устойчивого развития общества; информационного суверенитета и целостности государства
 - b) информации и информационных ресурсов ограниченного доступа; информационных систем, информационных технологий, средств связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц
 - c) права на производство, распространение, поиск, получение, передачу и использование информации; права на интеллектуальную собственность; права собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии
8. Принципы базовой системы защиты (установить соответствие)
- 1) Комплексный подход к построению системы защиты
 - 2) Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки
 - 3) Полнота контроля и регистрация попыток несанкционированного доступа
 - 4) Обеспечение надежности системы защиты
 - 5) Обеспечение контроля за функционированием системы защиты
 - 6) Экономическая целесообразность использования системы защиты
 - a) невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей
 - b) создание средств и методов контроля работоспособности механизмов защиты
 - c) стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае разработки и эксплуатации ИС без системы защиты информации
 - d) необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования
 - e) ведущую роль организационных мероприятий и оптимальное сочетание программно-аппаратных средств и организационных мер защиты
 - f) предоставление пользователям минимума строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автономной обработки доступной им конфиденциальной информации

Тема 6. Ответственность правонарушения информационной сфере

1. Информационное правонарушение определяется как
 - 1) общественно опасное (вредное), противоправное, виновное деяние (действия или бездействия) деликтоспособного лица, совершенное в информационной сфере и (или) с использованием информационных средств и технологий работы с информацией независимо от ее формы, либо в иной области человеческой деятельности в условиях информационной среды
 - 2) юридический факт (наряду с событием и действием), действия, противоречащие нормам права (антипод правомерному поведению)
 - 3) виновное общественно опасное деяние, запрещенное законодательством РФ под угрозой наказания, совершенное в области информационных правоотношений
2. Юридическая ответственность за информационные правонарушения - это
 - 1) применение к виновному лицу, совершившему правонарушение, мер воздействия, предусмотренных санкцией нарушенной нормы информационного права в определенном регламентированном порядке
 - 2) применение к виновному лицу, совершившему правонарушение, установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) и правил защиты информации, мер воздействия, предусмотренных санкцией нарушенной нормы информационного права в определенном регламентированном порядке
 - 3) ответственность работников, по вине которых предприятие, учреждение, организация понесли расходы по возмещению вреда
3. Состав информационного правонарушения включает в себя следующие элементы (признаки)
 - 1) объект, объективную сторону, субъект и субъективную сторону
 - 2) объект, субъект, поведение, право, обязанность, ответственность
 - 3) общественные отношения, физические и юридические лица, ответственность
4. Российская правовая система предусматривает следующие виды ответственности физических лиц за правонарушения в информационной сфере
 - 1) дисциплинарную (включая материальную), административную, гражданско-правовую (имущественную) и уголовную
 - 2) дисциплинарную (включая материальную), гражданско-правовую (имущественную) и уголовную
 - 3) дисциплинарную (включая материальную), административную, уголовную
5. Российская правовая система предусматривает следующие виды ответственности юридических лиц (предприятия, учреждения и организации) за правонарушения в информационной сфере
 - 1) административную и гражданско-правовую
 - 2) административную, гражданско-правовую и уголовную
 - 3) дисциплинарную (включая материальную), административную, гражданско-правовую (имущественную) и уголовную

6. К специальным признакам информационного правонарушения относятся (несколько вариантов)

- a) информационная сфера, информационная среда их совершения
- b) использование информационных средств и технологий
- c) противоправность, общественная опасность, деликтоспособность и виновность
- d) информационная сфера, противоправность, общественная опасность, деликтоспособность
- e) деликтоспособность и виновность

7. Информационное преступление это _____

8. Дисциплинарная ответственность предусматривает следующие меры наказания _____

Критерии оценки:

- **оценка «отлично»** выставляется студенту, если он ответил на 20-30 вопросов
- **оценка «хорошо»** выставляется студенту, если он ответил на 15-19 вопросов
- **оценка «удовлетворительно»** выставляется студенту, если он ответил на 10-14 вопросов
- **оценка «неудовлетворительно»** выставляется студенту, если он ответил меньше 10 вопросов

Темы эссе (рефератов, докладов, сообщений)

Тема 1. Основные понятия курса «Правовые основы информационной безопасности»

1. Понятие, структура и признаки информации с ограниченным доступом.
2. Понятие и виды вредной информации.

Тема 2. Информационная безопасность системе национальной безопасности РФ

3. Персональные данные и тайна частной жизни: общее и отличия.
4. Правовое регулирование электронной подписи
5. Правовое регулирование в сфере массовой информации
6. Правовое регулирование банковской тайны
7. Правовое регулирование государственной тайны
8. Правовое регулирование коммерческой тайны
9. Правовое регулирование рекламной деятельности

Тема 3. Правовые основы обеспечения информационной безопасности

- 10.Правовые основы защиты персональных данных
- 11.Уголовная ответственность за правонарушения в информационной сфере
- 12.Административная ответственность за правонарушения в информационной сфере

Тема 4. Организационное обеспечение информационной безопасности

- 13.Гражданко-правовая ответственность за правонарушения в информационной сфере.
- 14.Правовые проблемы борьбы со «спамом»
- 15.Электронные деньги: проблемы правового регулирования

Тема 5. Правовые режимы конфиденциальной информации

- 16.Правовое регулирование информационных технологий в области электронной коммерции
- 17.Правовое регулирование информационных технологий в области рекламы и маркетинга в Интернет
- 18.Правовое регулирование информационных технологий в области электронных банковских услуг

Тема 6. Ответственность правонарушения информационной сфере

- 19.Правовое регулирование информационных технологий в области электронного документооборота
- 20.Стандартизация, сертификация и лицензирование в информационной сфере

Методические рекомендации к написанию реферата

Реферат – краткое изложение в письменном виде содержания научных трудов по выбранной теме исследования. Это самостоятельная научно-исследовательская работа студента, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, делает выводы, обобщения.

Выбор темы реферата осуществляется преподавателем в рамках изучаемой дисциплины исходя из интересов студентов. Прежде чем выбрать тему реферата, студенту необходимо выяснить свой интерес, определить, над какой проблемой он хотел бы поработать, более глубоко ее изучить.

Цель реферата – приобретение студентами навыков самостоятельной работы по подбору, изучению, анализу и обобщению литературных источников.

Объем реферата составляет 7-12 страниц машинописного текста.

Процесс выполнения реферата состоит из следующих этапов.

- 1.Подбор литературы по избранной теме и ознакомление с выбранными источниками.

2. Составление плана реферата.

3. После заключения необходимо привести список литературы.

4. Оформление реферата. Текст работы должен быть набран на компьютере шрифтом TimesNewRoman размером 14 пт (при оформлении текста с использованием текстового процессора MicrosoftWord). Шрифт, используемый в иллюстративном материале (таблицы, графики, диаграммы и т.п.), при необходимости может быть меньше, но не менее 10 пт. Межстрочный интервал в основном тексте - полуторный. В иллюстративном материале межстрочный интервал может быть одинарным. Поля страницы должны быть:

- левое поле - 30 мм;
- правое поле - 10 мм;
- верхнее и нижнее поле - 20 мм.

Методические рекомендации к написанию эссе

Эссе – самостоятельная творческая письменная работа, по форме эссе обычно представляет собой рассуждение – размышление (реже рассуждение – объяснение), поэтому в нем используются вопросно-ответная форма изложения, вопросительные предложения, ряды однородных членов, вводные слова, параллельный способ связи предложений в тексте.

Особенности эссе:

- наличие конкретной темы или вопроса;
- личностный характер восприятия проблемы и ее осмысливания;
- небольшой объем;
- свободная композиция;
- непринужденность повествования;
- внутреннее смысловое единство;
- афористичность, эмоциональность речи.

Цель эссе состоит в развитии навыков самостоятельного творческого мышления и письменного изложения собственных мыслей. Писать эссе чрезвычайно полезно, поскольку это позволяет автору научиться четко и грамотно формулировать мысли, структурировать информацию, использовать основные категории анализа, выделять причинно-следственные связи, иллюстрировать понятия соответствующими примерами, аргументировать свои выводы; овладеть научным стилем речи.

Требования, предъявляемые к эссе:

1. Объем эссе не должен превышать 15–20 страниц
2. Эссе должно восприниматься как единое целое, идея должна быть ясной и понятной.
3. Необходимо писать коротко и ясно. Эссе не должно содержать ничего лишнего, должно включать только ту информацию, которая необходима для раскрытия вашей позиции, идеи.
4. Эссе должно иметь грамотное композиционное построение, быть логичным, четким по структуре.

5. Каждый абзац эссе должен содержать только одну основную мысль.
6. Эссе должно показывать, что его автор знает и осмысленно использует теоретические понятия, термины, обобщения, мировоззренческие идеи.
7. Эссе должно содержать убедительную аргументацию заявленной по проблеме позиции.

Критерии оценки рефератов и эссе:

оценка «отлично» - Соответствие целям и задачам дисциплины, актуальность темы и рассматриваемых проблем, соответствие содержания заявленной теме, заявленная тема полностью раскрыта, рассмотрение дискуссионных вопросов по проблеме, сопоставлены различные точки зрения по рассматриваемому вопросу, научность языка изложения, логичность и последовательность в изложении материала, количество исследованной литературы, в том числе новейших источников по проблеме, четкость выводов, оформление работы соответствует предъявляемым требованиям.

оценка «хорошо» - Соответствие целям и задачам дисциплины, актуальность темы и рассматриваемых проблем, соответствие содержания заявленной теме, научность языка изложения, заявленная тема раскрыта недостаточно полно, отсутствуют новейшие литературные источники по проблеме, при оформлении работы имеются недочеты.

оценка «удовлетворительно»- Соответствие целям и задачам дисциплины, содержание работы не в полной мере соответствует заявленной теме, заявленная тема раскрыта недостаточно полно, использовано небольшое количество научных источников, нарушена логичность и последовательность в изложении материала, при оформлении работы имеются недочеты.

оценка «неудовлетворительно»- Работа не соответствует целям и задачам дисциплины, содержание работы не соответствует заявленной теме, содержание работы изложено не научным стилем.

Вопросы к зачету

Модуль 1.

1. Понятие и признаки информации.
2. Информационная сфера и ее элементы.
3. Понятие безопасности и информационной безопасности.
4. Основные составляющие информационной безопасности.

5. Субъекты и объекты правоотношений в области информационной безопасности.
6. Понятие национальной безопасности.
7. Интересы личности в области информационной безопасности.
8. Интересы общества в области информационной безопасности.
9. Интересы государства в области информационной безопасности.
10. Понятие государственной информационной политики.
11. Основные положения государственной политики обеспечения информационной безопасности РФ.
12. Система обеспечения информационной безопасности РФ и ее основные функции.
13. Концептуальные положения организационного обеспечения информационной безопасности.
14. Понятие и виды угроз безопасности.
15. Угрозы информационной безопасности на объекте.
16. Организация службы безопасности объекта
17. Правовой режим информации: понятие, признаки, содержание.
18. Виды информации ограниченного доступа.
19. Требования, предъявляемые к организации защиты конфиденциальной информации.
20. Виды компьютерных преступлений.
21. Особенности квалификации компьютерных преступлений.
22. Преступления имущественного характера, которые совершаются с применением или в отношении средств компьютерной техники.

Модуль 2.

23. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.
24. Право и законодательство в сфере обеспечения информационной безопасности и их место в системе российского права из законодательства России.
25. Угрозы нарушения конфиденциальности, целостности, доступности информации.
26. Основные причины утечки информации.
27. Режим, правовой режим, правовой режим информации: определение.
28. Понятие правового режима информации и его основные признаки.
29. Понятие правового режима информации и его типовые элементы.
30. Характеристика видов правового режима информации с точки зрения его обязательности и объекта.
31. Общий правовой режим информации.
32. Специальные правовые режимы информации.
33. Тайна как специальный правовой режим.
34. Конфиденциальность как специальный правовой режим.
35. Государственная тайна и ее защита.

36. Защита персональных данных.
37. Защита коммерческой тайны.
38. Профессиональная тайна.
39. Служебная тайна.
40. Виды информационного законодательства, применяемые для регулирования отношений в Интернет.
41. Угроза безопасности, обеспечение безопасности: понятие.
42. Характеристика национальных интересов в Концепции национальной безопасности РФ.
43. Информационная безопасность: понятие, первоочередные меры по обеспечению, общие методы.
44. Информационная безопасность и информационные войны: понятие.
45. История информационных войн.
46. Информационная безопасность и информационное оружие: понятие.
47. Правонарушение и информационное правонарушение: определение, признаки, юридическая ответственность и основание привлечения к ответственности.
48. Состав информационного правонарушения.
49. Уголовная ответственность за информационное преступление.
50. Административная и гражданско-правовая ответственность в информационной сфере.

Критерии оценки:

- Оценка «зачтено» выставляется студенту, если ответы на поставленные вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Полно раскрываются причинно-следственные связи между явлениями и событиями. Делаются обоснованные выводы. Демонстрируются глубокие знания базовых нормативно-правовых актов. Соблюдаются нормы литературной речи.
- Оценка «не зачтено» выставляется студенту, если материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Не раскрываются причинно-следственные связи между явлениями и событиями. Не проводится анализ. Выводы отсутствуют. Ответы на дополнительные вопросы отсутствуют. Имеются заметные нарушения норм литературной речи.