Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»

Рабочая программа дисциплины
__Право информационной безопасности__
(наименование дисциплины в соответствии с учебным планом)

Набор 20_23_ г.

Направление подготовки/специальность __40.05.03 – «Судебная экспертиза»
(код и наименование)

Профиль подготовки/специализация: «Криминалистические экспертизы», «Экономические экспертизы»
(наименование)

Рабочая программа разработана в соответствии с требованиями ФГОС.

Разработчик (-и): __Бурмистрова Елена Сергеевна_
(

Рабочая программа рассмотрена и одобрена на заседании кафедры (протокол № _7_ «_20_» _марта__ 2023_г.).

Зав. кафедрой _Ловцов Дмитрий Анатольевич, д.т.н, профессор_ _____
(ФИО, ученая степень, ученое звание) (подпись)

Москва, 2023

ПРОТОКОЛ ИЗМЕНЕНИЙ
рабочей программы дисциплины
«Право информационной безопасности»
наименование дисциплины в соответствии с учебным планом
для набора ____ года на _____-_____уч.г.

Краткое содержание изменения	Дата и номер протокола заседания кафедры

Актуализация выполнена: _____
(ФИО, ученая степень, ученое звание)

_____ «__» _____ 20__г.
подпись

Зав. кафедрой _____
(ФИО, ученая степень, ученое звание)

_____ «__» _____ 20__г.
подпись

Оглавление

Аннотация рабочей программы дисциплины
«Право информационной безопасности»
Разработчик: Бурмистрова Елена Сергеевна

Цель изучения дисциплины	- формирование у студентов теоретических знаний умений, а также практических навыков юриста в област правового регулирования отношений в информационно сфере (далее – инфосфера) общественн производственной деятельности на основе глубоко исследования информационно-правовых пробле правового регулирования. - выработка у обучающихся навыков и умений п применению в практической деятельности полученны знаний по информационному праву, по реализации пра и законных интересов в информационной сфере.
Место дисциплины в структуре ППССЗ/ОПОП	Учебная дисциплина «Право информационной безопасности» – вариативная дисциплина, устанавливаемая вузом в цикле учебных дисциплин Б.1.ВД – «Информационно-правовой цикл» ФГОС ВПО по направлению подготовки 40.05.03 – «Судебная экспертиза».
Компетенции, формируемые в результате освоения дисциплины	**ОПК 5:** способность применять нормы материального и процессуального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.;
Содержание дисциплины	Тема 1. Классификация информационных технологий и информационных отношений в инфосфере. Тема 2. Анализ свойств и ограничений информационного ресурса (информации) СПР в правовых эргасистемах. Тема 3. Парадигма информационной безопасности эргасистем. Тема 4. Организационно-правовые аспекты информационно-криптографических технологий. Тема 5. Классификация и определение «информационного оружия. Тема 6. Анализ информационных правоотношения в инфосфере. Тема 7. Классификация тайн как объектов информационных правоотношений. Тема 8. Защита результатов интеллектуальной деятельности. Тема 9. Право на тайну.

	Тема 10. Ответственность за правонарушения в сфере информационной безопасности. Тема 11. Юридические фикции и проблемы их применения в праве информационной безопасности.
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет _3_ зачетных единиц _108_ часов.
Форма промежуточной аттестации	Зачёт

1.Цели и планируемые результаты изучения дисциплины

«Право информационной безопасности»

В процессе преподавания дисциплины «Право информационной безопасности» и его самостоятельного изучения студентами достигаются следующие **цели:**

— формирование у студентов основ знаний об информационной безопасности, роли и внедрении информации в современном обществе;

— формирование комплексных знаний об основных тенденциях развития технологий, связанных с обеспечением информационной безопасности;

— формирование практических навыков применения средств защиты информации при решении профессиональных задач.

В совокупности с другими дисциплинами ППССЗ/ОПОП дисциплина обеспечивает формирование следующих компетенций:

Таблица 1

№ п/п	Код компетенции	Название
1	ОПК-5	Способность применять нормы материального и процессуального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.

Планируемые результаты освоения дисциплины в части каждой компетенции указаны в картах компетенций по ППССЗ/ОПОП.

В рамках дисциплины осуществляется воспитательная работа, предусмотренная рабочей программой воспитания, календарным планом воспитательной работы.

2.Место дисциплины «Право информационной безопасности» в структуре ОПОП

Учебная дисциплина «Право информационной безопасности» – вариативная дисциплина, устанавливаемая вузом в цикле учебных дисциплин Б.1.ДВ – «Информационно-правовой цикл» ФГОС ВПО по направлению подготовки 40.05.03 – «Судебная экспертиза».

Интегрированный характер *права информационной безопасности* обусловливает необходимость при изучении данной учебной дисциплины определённой предварительной информационной подготовки (культуры) как студентов, так и самих преподавателей, а также знания основ различных смежных отраслей права: конституционного, гражданского, уголовного, административного, финансового, международного и др. Поэтому изучение дисциплины базируется на знаниях, полученных при освоении профильных естественнонаучных дисциплин «Информационные технологии в юридической деятельности» (формально-логические аспекты правового регулирования), «Информационные системы в профессиональной деятельности» и «Правовая информатика» (организационно-технические аспекты), а также общепрофессиональных дисциплин (правовые аспекты): «Теория государства и права», «Конституционное право РФ», «Гражданское право», «Уголовное право», «Административное право», «Финансовое право», «Трудовое право», «Международное публичное право», «Международное частное право», «Судоустройство».

В свою очередь она обеспечивает изучение таких дисциплин, как «Право СМИ», «Информационное право», «Международное информационное право».

3. Объем дисциплины «Право информационной безопасности» и виды учебной работы

Таблица 2.1

Вид учебной работы по **очной** форме обучения («Криминалистические экспертизы», «Экономические экспертизы»)	Трудоемкость	
	Зач. ед.	Час.
Общая трудоемкость дисциплины по учебному плану	3	108
Аудиторные занятия	0,9	32
Лекции	0,45	16
Практические занятия (семинары)	0,45	16
Самостоятельная работа	2,1	76
Форма промежуточной аттестации	Зачёт	

4. Содержание дисциплины «Право информационной безопасности»

4.1. Текст рабочей программы по темам

Введение

Объект, предмет, цель, задачи, актуальность, структура учебной дисциплины и отчётность. Основные нормативные правовые акты, руководящие документы и учебно-методическая литература. Место дисциплины «Основы (теоретические, организационно-технологические и правовые) информационной безопасности» в системе информационно-правовых наук

Понятие привилегированной информации (ресурса, товара, оружия), качества информации, защиты информации, информационной безопасности личности, общества и государства.

Раздел 1. Теоретические основы информационной безопасности в инфосфере

Тема 1. Классификация информационных технологий и информационных отношений в инфосфере.

Архитектура информационной сферы общественно-производственной деятельности и проблема информационной безопасности. Концептуально-логическая модель инфосферы (инфраструктура, среда, пространство). Взаимодействие базовых компонентов инфосферы.

Исходные методологические понятия (информация, безопасность, информационная безопасность, переработка информации в инфосфере).

Тема 2. Анализ свойств и ограничений информационного ресурса (информации) СПР в правовых эргасистемах.

Классификация (поколения) информационных технологий, «информационные революции». Концепция «новой информационной технологии». Принцип «автоформализации». Классификация информационных отношений в инфосфере, информационная борьба (война). Направления обеспечения информационной безопасности эргасистем.

Определение и классификация информации (виды, формы, атрибуты, качественные виды и формы проявления; формы представления) в эргасистеме.

Декомпозиция качества содержательной информации в эргасистеме: прагматические внутренние (*актуальность*) и внешние (*защищённость*) свойства. *Легитимность* информации (аутентичность, легальность, верифицируемость).

Тема 3. Парадигма информационной безопасности эргасистем.

Общенаучные информационные меры (Хартли, Шеннона). Апостериорный подход и примеры расчёта. Сравнительный анализ мер измерения (Хартли и Шеннона) количества информации (вывод формулы

Хартли из формулы Шеннона). Диаграмма Венна. Безусловные (априорные), условные (апостериорные) полные и частные, объединенная энтропии (логические операции над множествами).

Определение единицы измерения количества информации *Bit* (*двед*) на основе «двоичного канала коммуникации (связи). Скорость передачи информации и данных. Многократная телеграфия и достоверность информации.

Решение и анализ практических задач-примеров измерения количества информации: информационное содержание простого сообщения факта; прогнозирование в условиях информационной неопределённости; Геометрическая иллюстрация количества информации как снятой неопределённости.

Раздел 2. Организационно-технологические основы информационной безопасности в инфосфере

Тема 4. Организационно-правовые аспекты информационно-криптографических технологий.

Определения понятия «ценность информации». Принцип информационной ценности как принцип рациональной переработки информации в эргасистеме. Исходная концептуально-логическая модель (парадигма) информационной безопасности эргасистем.

Показатели эффективности обеспечения информационной безопасности эргасистем. Решение задач оценки ожидаемого безопасного времени. Решение задач оценки вероятности определения пароля по его отображениям. Формула Дж. Андерсона. Решение задач оценки скорости передачи информации при заданной скорости передачи данных.

Организационно-технологические аспекты информационно-криптографических технологий. Принципы (симметричность и ассиметричность) и способы криптографических преобразований информации: симметричное шифрование на основе обратимых функций Цезаря; симметричное шифрование на основе плохообратимых функций Шеннона; ассиметричное шифрование на основе плохообратимых функций Диффи, Хеллмана.

Организация защищённого информационного обмена в ИРС с применением ЭП.

Принципы обеспечения гарантированной информационной безопасности в эргасистеме. Условие совершенной (идеальной) информационно-криптографической скрытности передаваемых сообщений. Концепция гарантированной защиты информации, базирующаяся на принципе тотального контроля информационных каналов. Нетрадиционные (скрытые) информационные каналы доступа к ресурсам эргасистем.

Тема 5. Классификация и определение «информационного» оружия.

Понятие «информационного» оружия. Его применение и использование в «информационной» борьбе («информационной»

войне). Объекты воздействия информационного оружия. Применение информационного оружия на стратегическом, оперативном и тактическом уровнях.

Тема 6. Анализ информационных правоотношения в инфосфере.

Понятие информационных правоотношений. Состав, субъекты, объекты информационных правоотношений. Способы правового регулирования. Содержание информационных правоотношений (права, обязанности, ответственность).

Тема 7. Классификация тайн как объектов информационных правоотношений.

Понятие тайны. Виды тайн. Классификация. Законодательство, регулирующее вопросы тайн. Лица, органы и организации, обязанные обеспечить защиту сведений, составляющих соответствующий вид тайны. Состав и принципы формирования сведений, составляющих тайну. Отнесение сведений к соответствующему виду тайны.

Раздел 3. Правовые основы информационной безопасности в инфосфере

Тема 8. Защита результатов интеллектуальной деятельности.

Законодательство, регулирующее правоотношения в сфере интеллектуальной деятельности. Понятие результатов интеллектуальной деятельности. Средства и способы защиты.

Тема 9. Право на тайну.

Конституционные принципы обеспечения информационной безопасности. Виды информации, защищаемой законодательством РФ. Система и способы защиты государственной тайны. Конфиденциальная информация и её защита. Структура государственной системы защиты информации в РФ.

Законодательная база применения электронной подписи (ЭП): ГК РФ, ФЗ об информации, ЭП. Юридические свойства ЭП; условия равнозначности электронного документа и документа на бумажном носителе; условия юридической силы ЭП.

Классификация информационно-правовых режимов и юридически значимых видов тайн. Состав и структура целевого информационного правоотношения участников безопасного сетевого информационного обмена. Реляционная концептуально-логическая модель юридического понятия «тайна».

Тема 10. Ответственность за правонарушения в сфере информационной безопасности.

Понятие и виды ответственности. Законодательство, устанавливающее ответственность за правонарушения в сфере информационной безопасности.

Тема 11. Юридические фикции и проблемы их применения в праве информационной безопасности.

Анализ различных понятий данного термина, наличие фикций в информационном законодательстве Российской Федерации и в нормах международного права.

4.2. Разделы и темы дисциплины, виды занятий (тематический план)

Таблица 3

Тематический план

<u>очная</u> форма обучения

№ п/п	Раздел дисциплины, тема	Код компетенции	Общая трудоёмкость дисциплины	в том числе					Наименование оценочного средства
				Контактная работа	Самостоятельная работа под контролем преподавателя, НИРС	Занятия лекционного типа	Занятия семинарского типа	Практическая подготовка	
			час.	час.	час.	час.	час.	час.	
1	**Введение в дисциплину**			2	2	2	-		
2	**Раздел 1. Теоретические основы информационной безопасности в инфосфере**			**6**	**21**	**3**	**3**		Дискуссия, разноуровневые задачи и задания
	Тема 1. Классификация информационных технологий и информационных отношений в инфосфере	**ОПК-5**		2	7	1	1		Дискуссия, разноуровневые задачи и задания, доклад
	Тема 2. Анализ свойств и ограничений информационного ресурса (информации) СПР в правовых эргасистемах	**ОПК-5**		2	7	1	1		Дискуссия, разноуровневые задачи и задания, вопросы для семинара
	Тема 3. Парадигма информационной безопасности эргасистем	**ОПК-5**		2	7	1	1		Дискуссия, разноуровневые задачи и задания
3	**Раздел 2. Организационно-технологические основы**	**ОПК-5**		**9**	**29**	**4**	**5**		

	информационной безопасности в инфосфере								
	Тема 4. Организационно-правовые аспекты информационно-криптографических технологий	**ОПК-5**		2	8	1	1		Дискуссия, разноуровневые задачи и задания
	Тема 5. Классификация и определение «информационного» оружия	**ОПК-5**		2	7	1	1		Дискуссия, разноуровневые задачи и задания
	Тема 6. Анализ информационных правоотношения в инфосфере	**ОПК-5**		2	7	1	1		Дискуссия, разноуровневые задачи и задания
	Тема 7. Классификация тайн как объектов информационных правоотношений			3	7	1	2		Вопросы для семинаров, дискуссия
4	**Раздел 3. Правовые основы информационной безопасности в инфосфере**	**ОПК-5**		**11**	**28**	**5**	**6**		
	Тема 8. Защита результатов интеллектуальной деятельности	**ОПК-5**		2	8	1	1		Дискуссия, разноуровневые задачи и задания
	Тема 9. Право на тайну	**ОПК-5**		4	7	2	2		Дискуссия, разноуровневые задачи и задания, деловая игра
	Тема 10. Ответственность за правонарушения в сфере информационной безопасности	**ОПК-5**		3	7	1	2		Дискуссия, разноуровневые задачи и задания
	Тема 11. Юридические фикции и проблемы их применения в праве информационной безопасности	**ОПК-5**		2	6	1	1		Дискуссия, разноуровневые задачи и задания
Итого			**108**	**28**	**80**	**1 4**	**14**		

4.3. Самостоятельное изучение обучающимися разделов дисциплины

Таблица 4

№ раздела (темы) дисциплины	Вопросы, выносимые на самостоятельное изучение	Кол-во часов
Введение в дисциплину	Понятие привилегированной информации, качества информации, защиты информации, информационной безопасности личности, общества и государства.	2
1	История возникновения и развития информационного права.	7
2	Исторические аспекты развития информационно-криптографических технологий	7
3	Научное содержание общенаучной энтропийной концепции	7
4	Применение правовых норм по защите информации в судебном правоприменении	7
5	Применение ЭП в судебном правоприменении и в гражданско-правовых отношениях	7
6	Государственная политика в области информационной безопасности.	7
7	Конституционные основы и иные нормативные акты, регулирующие отношения в области государственной тайны.	7
8	Информационная война и информационное оружие. Концепция «информационной войны»	7
9	Иные аналоги собственноручной подписи и их правовой режим.	6
10	Применение информационно-правовых норм в уголовном судопроизводстве	6
11	Подготовка к семестровому творческому семинару «Системный подход и научно-приклад-ные проблемы эксперт-ной деятельности»	6
ИТОГО:		**76**

5. Учебно-методическое и информационное обеспечение дисциплины «Право информационной безопасности»

5.1. Учебно-методические рекомендации по изучению дисциплины «Право информационной безопасности»

Для освоения программы настоящей дисциплины студент должен

1. Знать:

- основные направления формирования и развития информационной инфраструктуры и единого информационного пространства России;
- основы формирования и использования информационного пространства в интересах органов государственной власти;

• содержание законодательного обеспечения формирования и развития единого информационного пространства России;

2. Уметь:

- находить необходимые нормативные правовые акты в системе действующего информационного и иного законодательства, регулирующие конкретные правоотношения в инфосфере, в том числе с использованием автоматизированных глоссариев правовой информации;

3. Иметь представление:

- о проблемах и перспективах развития отрасли.

Начинать изучение теоретического материала дисциплины следует с изучения компонентов[1] *информационной сферы* (информационная инфраструктура (информация, коммуникации, информационные системы), информационная среда, информационные средства, информационные технологии, информационное пространство – *объекты* информационных отношений. Информационные деятели – *субъекты* информационных отношений в инфосфер) и *информационно-правовых норм* Конституции Российской Федерации, включая *право на информацию*, порядок реализации права на информацию и гарантии предоставления информации.

Следует обратить внимание на следующие положения.

Информационное право – интегрированная отрасль российского права. Политико-правовая основа стратегии и принципы развития информационного общества в России. Понятие, объект, предмет, система, принципы, источники, способы, методы и средства права информационной безопасности. Место права информационной безопасности в системе российского права. Информационные права и свободы – фундамент информационного права. История становления и развития информационного права.

Информационные отношения и правоотношения в инфосфере – *объект* информационного права как науки, информационные правоотношения – как отрасли и учебной дисциплины. *Предмет* – способы и нормы правового регулирования информационных отношений (правоотношений) в инфосфере.

Принципы информационного права. Способы (императивный, диспозитивный) и средства правового регулирования, методы научных исследований в предметной области информационного права.

Правовые режимы информации. Понятия правового и информационно-правового режимов. Классификация информационно-правовых режимов. Правовые режимы информации неограниченного доступа (общедоступной информации). Правовые режимы информации ограниченного доступа. Правовые режимы информации обязательного предоставления[2] для доступа. Правовые режимы информации запрещённого ограничения доступа. Режим документированной информации.

---

[1] Изучаются в учебной дисциплине «Правовая информатика».

[2] В соответствии с федеральными законами РФ или с заключёнными соглашениями.

Юридическая ответственность за информационные правонарушения (преступления). Юридическая ответственность как самостоятельный институт информационного права. Понятие информационного правонарушения. Гражданско-правовая ответственность за информационные правонарушения. Основания для наступления гражданско-правовой ответственности. Договорная и деликтная ответственность. Административно-правовая ответственность за информационные правонарушения. Уголовная ответственность за преступления в инфосфере.

Ценность и качество содержательной информации. Классификация содержательной информации по роли, в которой она выступает в правовой эргасистеме и по доступу к ней. Общие (юридически значимые) внутренние (содержательность) и внешние (защищённость) свойства информации; специальные (правовые) свойства информации (легитимность, аутентичность, легальность, верифицируемость)[3].

Правовое обеспечение информационной безопасности. *Государственная политика в области информационной безопасности.* Информационная безопасность *как свойство объекта (личности, общества, государства, системы, эргасистемы и др.), характеризующее степень защищённости его потребностей в качественной (ценной) информации, необходимой для устойчивой жизнедеятельности (функционирования) и развития (обучения), включая защищённость его интересов от преднамеренных угроз в инфосфере*.

Управление информационной безопасностью личности, общества и государства. Место информационной безопасности в системе национальной безопасности. Структурно-феноменологическая модель и иерархия потребностей личности. Обеспечение информационной безопасности в условиях информационной борьбы (войны). Классификация и роль «информационного оружия». Проблема защиты от «организационного оружия». Новые организационные технологии.

Правовое регулирование отношений в области государственной тайны. Конституционная основа института государственной тайны. Цели правового регулирования отношений, связанных с государственной тайной. Основные *объекты* информационных правоотношений (государственная тайна; носители сведений, составляющих государственную тайну; допуск к государственной тайне; доступ к сведениям, составляющим государственную тайну; гриф секретности; средства защиты информации; перечень сведений, составляющих государственную тайну). Основные *субъекты* информационных правоотношений в сфере государственной тайны (органы законодательной, исполнительной и судебной власти, местного самоуправления; организации, учреждения и предприятия независимо от их организационно-правовой формы и формы собственности; должностные лица и граждане РФ, взявшие на себя обязательства, либо обязанные по

[3] Изучаются в учебной дисциплине «Правовая информатика».

своему статусу исполнять требования законодательства РФ о государственной тайне; система защиты государственной тайны). *Полномочия* органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты. Перечень сведений, составляющих государственную тайну. Отнесение сведений к государственной тайне и засекречивание этих сведений. Рассекречивание сведений и их носителей. Распоряжение сведениями, составляющими государственную тайну. Защита государственной тайны. Контроль и надзор за обеспечением защиты государственной тайны. Ответственность за разглашение государственной тайны. Защита информации от несанкционированного доступа по традиционным и нетрадиционным[4] (скрытым) информационным каналам.

Правовое регулирование отношений в области коммерческой тайны. Конституционная основа института коммерческой тайны. Цели правового регулирования информационных правоотношений при работе с информацией, составляющей коммерческую тайну. Основные *объекты* правоотношений (информация, составляющая коммерческую тайну; информация, которая не может составлять коммерческую тайну; режим коммерческой тайны, носители коммерческой тайны, разглашение коммерческой тайны, неправомерные способы получения коммерческой тайны). *Субъекты* информационных правоотношений (создатель или производитель коммерческой тайны, обладатель коммерческой тайны, конфидент коммерческой тайны, работодатель, работник, органы государственной власти и местного самоуправления). Установление режима коммерческой тайны. Отнесение сведений к коммерческой тайне. Правомерное получение и использование информации, составляющей коммерческую тайну. Охрана коммерческой тайны в трудовых отношениях. Защита прав на коммерческую тайну. Ответственность за нарушения при работе с коммерческой тайной.

Правовое регулирование отношений в области персональных данных. Конституционные основы института персональных данных. Цели правового регулирования отношений, возникающих при работе с персональными данными.

Основные *объекты* информационных правоотношений (персональные данные, перечень персональных данных, массив персональных данных, режим конфиденциальности персональных данных, согласие субъекта данных, работа с персональными данными). *Субъекты* информационных правоотношений (субъект персональных данных, держатель (обладатель)

---

[4] ***Нетрадиционный информационный канал*** (*unusual channel, covert channel, subliminal channel*) – несанкционированный *способ* скрытой *передачи* не *легитимной информации* по действующим («традиционным») *каналам связи*, нарушающий системную *политику безопасности*. *Например*, способ временной модуляции санкционированного *приёма* потоков различной внутрисистемной информации, осуществляемой принимающим *абонентом* (высокого уровня *конфиденциальности*) и распознаваемой («детектируемой») передающим абонентом (низкого уровня конфиденциальности), в результате чего в обратном направлении как бы скрытно передаётся нелегитимная информация (*например*, секретный *шифр*).

массива персональных данных, оператор персональных данных, третье лицо, получатель персональных данных, органы государственной власти и местного самоуправления). Права субъекта персональных данных, ограничение прав субъектов на свои персональные данные. Права и обязанности держателя (обладателя) и оператора по работе с массивами персональных данных. Уполномоченный по правам субъектов персональных данных.

Государственное регулирование работы с персональными данными. Основные принципы работы с персональными данными, условия законности работы с персональными данными. Общедоступные массивы персональных данных. Специальные категории персональных данных. Ответственность за правонарушения при работе с персональными данными.

Правовые проблемы в сфере электронного документооборота. Понятие электронного документа. Правовой режим электронного документа. Правовые условия использования электронного документооборота.

Понятия и применение электронной подписи (простой, усиленной, квалифицированной – КЭП), закрытого и открытого ключей КЭП (аналога электронной цифровой подписи – ЭП), средств КЭП, удостоверяющего центра. Требования, предъявляемые к удостоверяющим центрам. Смысл криптографических преобразований информации. Принципы организации защищённого обмена в автоматизированной информационной системе (сети). Правовой режим КЭП.

Основные *объекты* информационных правоотношений (персональные данные, перечень персональных данных, массив персональных данных, режим конфиденциальности персональных данных, согласие субъекта данных, работа с персональными данными). *Субъекты* информационных правоотношений (субъект персональных данных, держатель (обладатель) массива персональных данных, оператор персональных данных, третье лицо, получатель персональных данных, органы государственной власти и местного самоуправления). Права субъекта персональных данных, ограничение прав субъектов на свои персональные данные. Права и обязанности держателя (обладателя) и оператора по работе с массивами персональных данных. Уполномоченный по правам субъектов персональных данных.

Государственное регулирование работы с персональными данными. Основные принципы работы с персональными данными, условия законности работы с персональными данными. Общедоступные массивы персональных данных. Специальные категории персональных данных. Ответственность за правонарушения при работе с персональными данными.

При обсуждении наиболее актуальных (базовых) тем и вопросов семинаров студент должен быть готов принять активное участие в «мозговом штурме», оперативно генерируя предложения и выводы, подкреплённые примерами (выдержками) из изученной рекомендованной специальной, учебной и научной литературы.

Деловая игра – форма занятия, имитирующего реальные условия, в ходе которого отрабатываются конкретные специфические операции, моделируется соответствующий рабочий процесс. В условиях имитации реальных условий происходит формирование профессиональных компетенций при отработке конкретных специфических операций.

Для проведения деловой игры необходим подготовительный этап: разработка сценария, плана, общего описания игры, содержание инструктажа по ролям, разработка творческих заданий, связанных с будущей профессией, используемыми экспертными технологиями, подготовка материального обеспечения.

Успех семинара в значительной мере зависит от степени его подготовленности. Во время подготовки должны быть решены вопросы содержательного, методического, дидактического и организационного характера. Прежде всего необходимо определить темы. Они должны быть актуальными и злободневными. Занятия должны быть связаны с типичными ситуациями, с которыми могут столкнуться эксперты и специалисты в будущей своей профессиональной деятельности.

К каждой игре надлежит разработать сценарный план и сценарий, в котором содержится информация об игровых ролях, их описание, правила игры. Сценарием должно быть обеспечено взаимодействие игроков. По существу, деловая игра- это своеобразный спектакль, в котором должны быть расписаны роли, отдельно подготовлены объекты криминалистического анализа – научного спора.

Ввод в игру осуществляется посредством постановки проблемы, цели, знакомства с правилами, регламентом, распределением ролей, формированием групп, консультации. Студенты делятся на несколько малых групп. Количество групп определяется числом практических заданий (кейсов), которые будут обсуждаться в процессе занятия и количеством ролей. Малые группы формируются либо по желанию студентов, либо по указанию преподавателя. Малые группы занимают определенное пространство, удобное для обсуждения на уровне группы. Каждая малая группа обсуждает практическое задание в течение отведенного времени. Задача данного этапа – сформулировать групповую позицию по практическому заданию.

Следует обратить внимание еще на одну деталь. Если в ходе игры обнаруживается явное преимущество или слабость какой-либо из групп, целесообразно тактично провести перегруппировку, поменять состав, «усилить» или «разбавить» одну или несколько из них.

На этапе проведения деловой игры осуществляется работа над заданием, межгрупповая дискуссия, защита результатов. Заслушиваются суждения, предлагаемые каждой малой группой, с учетом предложенной роли. Здесь следует иметь в виду, что существуют оптимальные «зоны» для общения. Согласно психологическим исследованиям, социальная дистанция, на которой «делаются дела», имеет две фазы – близкую (120-210 см) и

далекую (210-360 см). Это означает, что дистанция между участниками игры не должна быть значительной. Уменьшение дистанции вызывает у участников эффект доверия, приводит к большей открытости в общении и вызывает положительные эмоции.

Игровой материал и объекты должны быть заранее скомпонованы, тиражированы и представлены в необходимом количестве, разложены по тематике, стадиям проведения игры, подготовлена справочная литература.

Преподаватель должен не только знать материал, но и уметь вести игру, контролировать игровой режим, быть готовым мгновенно реагировать на неожиданно возникающие в игре ситуации и сбои.

Игру следует вести эмоционально, заинтересованно, но ни в коем случае не принимать решение за играющих, не подсказывать наиболее целесообразное решение.

Во время игры вырабатываются и принимаются решения в условиях поэтапного и многошагового уточнения необходимых факторов, анализа информации, дополнительных сведений, поступающих и вырабатываемых на отдельных ее этапах. Ставятся частные задачи, дается развитие ситуации. На первом этапе игры формулируется ее цель, участники должны уяснить смысл и содержание заданий. На втором этапе преподаватель организует коллективное обсуждение, где каждый может и должен высказать свою точку зрения. Такое обсуждение выявляет разные подходы решения одной и той же проблемы.

На следующем этапе организуется межгрупповая дискуссия. В группе выбирается спикер, который озвучивает позицию группы. Каждая группа предлагает свой вариант решения рассматриваемой проблемы, соглашаясь или опровергая аргументацию иных выступающих. Затем выступают участники, имеющие особое мнение. В ходе активной дискуссии оппоненты задают вопросы, выступают с аргументированной критикой, обосновывая свою точку зрения ссылками на законодательство, научные или практические данные.

Преподаватель задает тон дискуссии, демонстрирует способность к пониманию, готовность включиться к обсуждению любой точки зрения, т.е. занимает позицию «беспристрастной заинтересованности».

Преподавателю необходимо обеспечить успешность и плодотворность обсуждения, зафиксировать внимание студентов, что в ходе дискуссии необходимо умение не только говорить, но и внимательно слушать.

Особое внимание следует уделить подведению итогов. В завершении преподаватель формулируется общее мнение, выражающее совместную позицию по практическому заданию. Преподаватель дает оценочное суждение по работе каждой группы, по решению практических заданий (кейсов) с учетом предложенных ролей, и эффективности предложенных путей решения; дает экспертную оценку выявленным правонарушениям и аргументирует правильность или ошибочность выводов экспертов.

Преподавателю необходимо тактично показать, чего удалось добиться участникам игры, какие ошибки при этом были допущены.

В случае возникновения затруднений при изучении той или иной темы студенту рекомендуется обратиться к преподавателю за разъяснением в аудитории или индивидуально – после занятий, в часы консультаций или по электронной почте.

При подготовке к групповым занятиям и семинарам следует:

- изучить всю рекомендованную специальную, учебную и научную литературу кафедры;
- законспектировать рекомендованные нормативные правовые акты;
- разработать компьютерную презентацию сообщения (доклада).

5.2. Перечень нормативных правовых актов, актов высших судебных органов, материалов судебной практики

1. **Закон о ГАС «Выборы»** – Федеральный закон от 10 января 2003 г. № 20-ФЗ «О государственной автоматизированной системе «Выборы» // СЗ РФ. – 2003. – № 2. – Ст. 172.

2. **Закон об информации** – Федеральный закон[5] от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. – 2006. – 29 июл.

3. **Стратегия развития информационного общества** – Стратегия развития информационного общества в Российской Федерации, утверждённая Указом Президента РФ от 9 мая 2017 г. № 203 // СЗ РФ. 2017. № 20. Ст. 2901.

4. **Программа** «**Электронная Россия»** – Федеральная целевая программа «Электронная Россия на 2002 – 2010 годы», утверждённая Постановлением Правительства РФ от 28 января 2002 г. № 65 // СЗ РФ. – 2002. – № 5. – Ст. 122.

5. **Программа «Цифровая экономика»** – Распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» / «КонсультантПлюс».

6. **ГОСТ АСУ** – ГОСТ 24.003–84, 24.101–80, 24.103–84, 24.104–85, 24.201–85, 24.205–80, 24.301–80, 24.302–80, 24.303–80, 24.304–82. АСУ. Основные положения. Термины и определения. Общие требования. Техническое задание на АСУ. Условные обозначения. – М.: Стандарты, 1988.

5.3. Информационное обеспечение изучения дисциплины «Право информационной безопасности»

[5] Статья 11, п. 3 (юридическая сила ЭД, ЭЦП).

Информационные, в том числе электронные ресурсы Университета, а также иные электронные ресурсы, необходимые для изучения дисциплины:

№ п./п.	Наименование	Адрес в сети Интернет
1	ZNANIUM.COM	http://znanium.com Основная коллекция Коллекция издательства Статут Znanium.com. Discovery для аспирантов
2	ЭБС ЮРАЙТ	www.biblio-online.ru
3	ЭБС «BOOK.ru»	www.book.ru коллекция издательства Проспект Юридическая литература ; коллекции издательства Кнорус Право, Экономика и Менеджмент
4	НЦР РУКОНТ	http://rucont.ru/ Раздел Ваша коллекция - РГУП-периодика (электронные журналы)
5	Информационно-образовательный портал РГУП	www.op.raj.ru электронные версии учебных, научных и научно-практических изданий РГУП
6	Система электронного обучения «Фемида»	www.femida.raj.ru Учебно-методические комплексы, Рабочие программы по направлению подготовки
7	Правовые системы	Гарант, Консультант
8	иное по необходимости	…

Основная и дополнительная литература указана в Карте обеспеченности литературой.

6. Материально-техническое обеспечение

Для материально-технического обеспечения дисциплины используются специальные помещения. Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования.

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие рабочим

программам дисциплин. Демонстрационное оборудование представлено в виде мультимедийных средств. Учебно-наглядные пособия представлены в виде экранно-звуковых средств, печатных пособий, слайд-презентаций, видеофильмов, макетов и т.д., которые применяются по необходимости в соответствии с темами (разделами) дисциплины.

Для самостоятельной работы обучающихся помещения оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.

Перечень специальных помещений ежегодно обновляется и отражается в справке о материально-техническом обеспечении основной образовательной программы.

Состав необходимого комплекта лицензионного программного обеспечения ежегодно обновляется, утверждается и отражается в справке о материально-техническом обеспечении основной образовательной программы.

37	Право информационной безопасности	Компьютерный класс: 15 оборудованных компьютерами рабочих мест, выход в сеть Интернет, учебная доска, стол преподавателя, учебно-наглядные пособия	394006, Воронежская область, г. Воронеж, Ленинский район, ул. 20-летия Октября, дом 95, этаж 2, каб. 315	Оперативное управление	Свидетельство о государственной регистрации права серия 36-АД № 699874 от 04.12.2014г. Бессрочно

Специальные помещения - учебные аудитории для проведения занятий всех видов, предусмотренных ОПОП, оснащены наборами мультимедийного демонстрационного оборудования (компьютер с программным обеспечением, проектор, акустическая система) и учебно- наглядными пособиями, обеспечивающими тематическое иллюстрирование учебного процесса (слайд-презентации лекций, видеофильмы, видеоролики и т.п.)

7. Карта обеспеченности литературой

Направление подготовки: 40.05.03 – «Судебная экспертиза»
Профиль: «Криминалистические экспертизы», «Экономические экспертизы»
Дисциплина «Право информационной безопасности»
Курс 3

Наименование, Автор или редактор, Издательство, Год издания, кол-во страниц	Вид издания	
	ЭБС (указать ссылку)	Кол-во печатных изд. в библиотеке вуза
1	2	3
Основная		
Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927	https://urait.ru/book/informacionnaya-bezopasnost-i-zaschita-informacii-530927	1

Ловцов Д.А. Теория защищенности информации в эргасистемах: Монография М.: РГУП, 2021, 276 стр. ISBN: 978-5-93916-896-0	https://op.raj.ru/serijnye-izdaniya/103-monografii/1017-lovcov-teor-zash	
Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 427 с. — (Высшее образование). — ISBN 978-5-534-18043-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/534187	https://urait.ru/book/informacionnoe-pravo-534187	
Под ред. Поляковой Т. А., Стрельцова А. А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239 (дата обращения: 06.06.2023).	https://urait.ru/book/organizacionnoe-i-pravovoe-obespechenie-informacionnoy-bezopasnosti-511239	
Дополнительная		
Русскевич, Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : учебное пособие / Е.А. Русскевич. — 2-е изд., доп. — Москва : ИНФРА-М, 2023. — 188 с. — (Высшее образование: Магистратура). - ISBN 978-5-16-014392-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1993603 (дата обращения: 06.06.2023).	https://znanium.com/catalog/document?id=428649#bib	-
Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. - Москва : Директ-Медиа, 2020. - 270 с. - ISBN 978-5-4499-0496-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1908082	https://znanium.com/catalog/document?id=418610#bib	1
Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации : учебник / сост. И. Г. Дровникова, А. В. Калач, И. И. Лившиц [и др]. - Воронеж : Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1999941 (дата обращения: 06.06.2023).	https://znanium.com/catalog/document?id=426504#bib	
Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1359091	https://znanium.com/catalog/document?id=375641#bib	1

Вострецова, Е. В. Основы информационной безопасности : учебное пособие / Е. В. Вострецова. - Екатеринбург : Изд-во Уральского ун-та, 2019. - 204 с. - ISBN 978-5-7996-2677-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1936350	https://znanium.com/catalog/document?id=422383#bib	

Зав. библиотекой _____ Зав. кафедрой_____

8. Фонд оценочных средств

8.1. Паспорт фонда оценочных средств по дисциплине «Право информационной безопасности»

№ п/п	Раздел дисциплины, тема	Код компетенции	Наименование оценочного средства
1.	1- 11	**ОПК-5** Способность применять нормы материального и процессуального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.	доклад, сообщение, реферат, вопросы для семинаров, деловая игра, дискуссия

8.2. Оценочные средства

Деловая (ролевая) игра

Перечень компетенций (части компетенции), проверяемых оценочным средством:

ОПК 5: способность применять нормы материального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.

Тема «Сравнительный анализ проблем применения программных продуктов, реализующих различные криптографические алгоритмы, используемые в системах защиты информации в глобальных компьютерных сетях.»

Концепция: Анализ проблем применения программных продуктов двумя-тремя группами экспертов с последующим сравнением результатов.

№ п/п	Вопросы	Код компетенции (части компетенции)
1	Реализовать алгоритм криптографического закрытия информации методом гаммирования, в качестве гаммы использовать случайную последовательность, получаемую с помощью генератора случайных чисел..	ОПК-5
2	Реализовать алгоритм криптографического закрытия информации методом перестановок, ключевая информация должна быть варьируемой пользователем через соответствующий интерфейс. Получение коллективного (обобщенного) мнения экспертной группы.	ОПК-5
3	Реализовать алгоритм криптографического закрытия	ОПК-5

	информации методом стеганографии Выявление подгрупп экспертов с близкими мнениями.	
4	Реализовать алгоритм криптографического закрытия информации методом последовательно подстановки и последующей перестановки.	ОПК-5

Роли:

1. Заказчик аналитического обзора.
2. Руководители групп экспертов.
3. Члены экспертных групп.

Ожидаемый результат:

овладение студентами методами, приемами и навыками сравнительного анализа проблем применения программных продуктов, реализующих различные криптографические алгоритмы, используемые в системах защиты информации.

Методические рекомендации по проведению «Деловой игры».

К игре надлежит разработать сценарный план и сценарий, в котором содержится информация об игровых ролях, их описание, правила игры. Сценарием должно быть обеспечено взаимодействие игроков. По существу, деловая игра – это своеобразный спектакль, в котором должны быть расписаны роли, отдельно подготовлены объекты криминалистического анализа – научного спора.

Ввод в игру осуществляется посредством постановки проблемы, цели, знакомства с правилами, регламентом, распределением ролей, формированием групп, консультации. Студенты делятся на несколько малых групп. Количество групп определяется числом практических заданий (кейсов), которые будут обсуждаться в процессе занятия и количеством ролей. Малые группы формируются либо по желанию студентов, либо по указанию преподавателя. Малые группы занимают определенное пространство, удобное для обсуждения на уровне группы. Каждая малая группа обсуждает практическое задание в течение отведенного времени. Задача данного этапа – сформулировать групповую позицию по практическому заданию.

Организуется межгрупповая дискуссия.

Критерии оценки[*]:

Критерии	**Баллы**
Студент дает правильные ответы на 90-100 % заданий	*2*
Студент дает правильные ответы на 70-90 % заданий	*1.5*
Студент дает правильные ответы на 50-70 % заданий	*1*
Студент дает правильные ответы на менее 50 % заданий	*менее 1*

[*] *Критерии оценки могут быть индивидуальны для каждой деловой игры*

Вопросы для занятий семинарского типа (семинаров, коллоквиумов)

Перечень компетенций (части компетенции), проверяемых оценочным средством (наименование, код):

ОПК 5: способность применять нормы материального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.

Тема 1. Тематический творческий семинар «Архитектура информационной сферы ОПД и проблема информационной безопасности»

№ п/п	Вопросы	код компетенции (части компетенции)
1.	Предпосылки формирования информационного права.	ОПК-5
2.	Понятие и структура инфосферы	ОПК-5
3.	Проблемы информационной безопасности	ОПК-5

Тема 2. Законодательство в сфере информационной безопасности

№ п/п	Вопросы	код компетенции (части компетенции)
1.	Понятие законодательства в сфере информационной безопасности и его система.	ОПК-5
2.	Доктрина информационной безопасности РФ.	ОПК-5
3.	Информационно-правовые нормы Конституции Российской Федерации.	ОПК-5
4.	Информационное обеспечение государственной политики РФ.	ОПК-5

Тема 3. Юридическая ответственность за правонарушения в сфере информационной безопасности

№ п/п	Вопросы	код компетенции (части компетенции)
1.	Понятие и виды ответственности за	ОПК-5

	правонарушения в сфере информационной безопасности	
2.	Гражданско-правовая ответственность за правонарушения в сфере информационной безопасности	ОПК-5
3.	Административно-правовая ответственность за правонарушения в сфере информационной безопасности	ОПК-5
4.	Уголовная ответственность за преступления в сфере информационной безопасности	ОПК-5

Тема 4. Тематический творческий семинар с привлечением экспертов «Правовые основы информационной безопасности личности, общества и государства»

№ п/п	Вопросы	код компетенции (части компетенции)
1.	Понятие и предмет информационной безопасности и ее место в системе обеспечения национальной безопасности.	ОПК-5
2.	Основы теории интересов. Национальные интересы России в информационной сфере: для личности, общества и государства.	ОПК-5
3.	Принципы, задачи, функции и структура обеспечения информационной безопасности.	ОПК-5
4.	Угрозы информационной безопасности РФ.	ОПК-5
5.	Право и законодательство в сфере обеспечения информационной безопасности и их место в системе российского права и законодательства России	ОПК-5
6.	Правовое регулирование отношений в области государственной тайны.	ОПК-5
7.	Правовое регулирование отношений в сфере конфиденциальной информации	ОПК-5

Тема 5. Тематический творческий семинар «Теоретические и организационно-технологические основы информационной безопасности в инфосфере»

№ п/п	Вопросы	код компетенции (части компетенции)
1	Защита информационных ресурсов от несанкционированного доступа.	ОПК-5
2	Международное сотрудничество РФ в области защиты информации.	ОПК-5
3	Понятия и применение электронной подписи	ОПК-5
4	Иные аналоги собственноручной подписи и их правовой режим	ОПК-5

Тема 6. Тематический творческий семинар «Правовые основы информационной безопасности в инфосфере»

№ п/п	Вопросы	код компетенции (части компетенции)
1	Информационно-психологическая война.	ОПК-5
2	Информационно-психологическое оружие.	ОПК-5
3	Правовые проблемы в сфере Интернета и других глобальных сетей	ОПК-5

Критерии оценивания:

Критерии	**Баллы**
Частичное владение учебным материалом по рассматриваемому вопросу и/или ссылки только на не рекомендованную литературу.	1
Владение основными положениями учебного материала по рассматриваемому вопросу и/или ссылки только на дополнительную рекомендованную и на не рекомендованную литературу.	2
Общее владение учебным материалом по рассматриваемому вопросу и/или ссылки только на дополнительную рекомендованную литературу.	3
Свободное владение учебным материалом по	4

рассматриваемому вопросу, ссылки на основную рекомендованную литературу.	
Свободное владение учебным материалом по рассматриваемому вопросу, ссылки на основную рекомендованную литературу, наличие компьютерной презентации.	5

Комплект заданий для контрольной работы

1. Перечень компетенций (части компетенции), проверяемых оценочным средством (наименование, код):

ОПК 5: способность применять нормы материального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.

№ п/п	Тема	Код компетенции
1.	Понятие и признаки электронного документа, правовое регулирование в сфере электронного документооборота.	ОПК-5
2.	Понятия и юридические свойства электронной подписи, проблемы применения электронной цифровой подписи в Российской Федерации.	ОПК-5
3.	Информационная безопасность в условиях функционирования в России глобальных сетей.	ОПК-5
4.	Правовые проблемы охраны персональных данных, охрана персональных данных в трудовых отношениях.	ОПК-5
5.	Правовые режимы информации ограниченного доступа, юридическое понятие тайны, классификация и правовая характеристика видов тайн.	ОПК-5
6.	Структура системы правового обеспечения информационной безопасности, правовой статус субъекта персональных данных.	ОПК-5
7.	Понятие, направления и задачи реализации концепции электронного правительства в Российской Федерации, правовые проблемы охраны государственной тайны.	ОПК-5
8.	Охрана коммерческой тайны, правовые проблемы охраны коммерческой тайны в трудовых отношениях.	ОПК-5
9.	Правовые вопросы обеспечения информационной безопасности, компьютерные преступления как угроза экономической безопасности личности,	ОПК-5

	общества и государства.	
10.	Международные стандарты информационного обмена.	ОПК-5
11.	Правовые проблемы использования информационно-компьютерных технологий в экономике, правовой режим документированной информации.	ОПК-5
12.	Информационные правоотношения как особый род общественных правоотношений, право граждан на информацию о деятельности органов государственной власти и управления.	ОПК-5
13.	Правовые проблемы в сфере глобальной телекоммуникационной сети Интернет и безопасность информации.	ОПК-5
14.	Основные проблемы информатизации юридической деятельности, ГАС «Правосудие».	ОПК-5
15.	Правовое регулирование в области использования персональных данных, соблюдение прав пользователей сетевых сервисов.	ОПК-5
16.	Концепция информационной безопасности.	ОПК-5
17.	Проблемы и способы международно-правового обеспечения глобального информационного обмена, понятие и классификация «информационного оружия». Угрозы его применения.	ОПК-5
18.	Особенности неправомерного доступа к «компьютерной» информации, проблемы юридической квалификации и пути их решения.	ОПК-5
19.	Модель информационной безопасности судебных автоматизированных систем: правовое регулирование и юрисдикция.	ОПК-5
20.	Принципы создания единой правовой нормативно-методической базы автоматизированных систем судопроизводства. Классификация судебной информации.	ОПК-5

Критерии оценивания:

Критерии	**Баллы**
Тема не раскрыта и/или оформление не соответствует требованиям ФОС.	0
Тема раскрыта недостаточно полно (отсутствуют творческие выводы).	3
Тема раскрыта, творческие выводы сделаны, но имеются погрешности в оформлении.	5
Тема раскрыта, творческие выводы сделаны, оформление соответствует требованиям Университета.	7
Тема раскрыта, творческие выводы сделаны, оформление соответствует требованиям Университета. Выступление с результатами на семинаре с компьютерной презентацией.	10

Комплект разноуровневых задач/заданий

1. Перечень компетенций (части компетенции), проверяемых оценочным средством (наименование, код):

   ОПК 5: способность применять нормы материального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.

Задачи репродуктивного уровня

№ п/п	Задание	Код компетенции (части) компетенции
1.	Редакция журнала «Hello» обратилась с письменным запросом к директору супермаркета «Азбука вкуса». В данном запросе, в частности, требовалось ответить на следующие вопросы: 1. Изменился ли объем продаж сигарет после вступления в силу закона о запрете курения в общественных местах? 2. Каким образом продавцы данного супермаркета определяют возраст (совершеннолетие) покупателей? Руководитель супермаркета проигнорировал данный запрос. На повторный запрос, поступившем на следующий день, он, по прошествии 5 дней в письменном ответе указал, что не может предоставить данные сведения, поскольку они составляют коммерческую тайну, также он ненавязчиво отметил, что, поскольку его брат работает в суде секретарем судебного заседания, то данные сведения могут считаться не только коммерческой, но и государственной тайной. *1. Какие меры ответственности могут быть применены к руководителю супермаркета (с опорой на Закон РФ от 27.12.1991 N 2124-1 (ред. от 25.11.2017) "О средствах массовой информации")?* *2. Прав ли был руководитель супермаркета? (В части мотивирования своего отказа)* *3. Какие данные могут составлять коммерческую тайну (Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне")?*	ОПК-5
2	Сотрудник Главного управления	ОПК-5

	Генерального штаба Вооружённых Сил Российской Федерации Мишин по своим обязанностям, часто выезжал заграницу для проведения официальных встреч и переговоров. По службе имел 1 форму допуска к государственной тайне. Однажды, в ходе дружественной беседы с дипломатами иностранного государства он согласился предоставить сведения, составляющие государственную тайну, в обмен на защиту этим государством его семьи и предоставления ему большой суммы денежных средств. Ему было поручено предоставить сведения о размещении атомных ракетных подводных лодок Российской Федерации в морском пространстве агенту иностранной спецслужбы, находящемуся в Российской Федерации. Через 18 дней он получил данные сведения, вынес копии документов и схем за территорию Управления и в назначенном месте осуществил встречу с иностранным агентом с целью передачи ему секретной информации. В ходе передачи документов был задержан сотрудниками Управления Военной Контрразведки ФСБ России. *Под какую статью УК РФ попадают действия Мишина?*	

Задачи реконструктивного уровня

№ п/п	Задание	Код компетенции (части) компетенции
1.	Егоров В.И. работая в правоохранительных органах, имеет допуск к сведениям, составляющим государственную тайну. Как-то раз, отвечая на вопросы журналистки Волковой Е.Г., непроизвольно разгласил сведения, составляющие государственную тайну, вскоре данная информация была опубликована в газете «Октябрь». *1.Определить круг правоотношений, возникающих в задаче и нормы права, которыми регулируются данные правоотношения.* *2. Можно ли привлечь Егорова В.И и Волкову*	ОПК-5

	Е.Г. к ответственности, если да, то к какому виду? Обоснуйте свой ответ.	
2.	Современная металл-группа «Жираф» была запрещена на территории Российской Федерации. Текста и атрибутика данного музыкального коллектива содержали текста атеистической направленности и вызывали громкий общественный резонанс при гастролировании по России. Через 2 дня после начала гастролей данная группа была депортирована и получила запрет на выступления на территории РФ на основании решения суда. *Правомерно ли решение суда?*	ОПК-5

Задачи творческого уровня

№ п/п	Задание	Код компетенции (части) компетенции
1.	Эдвард Джозеф Сноуден — американский технический специалист и бывший сотрудник ЦРУ и Агентства национальной безопасности (АНБ) США. В начале июня 2013 года Сноуден передал газетам The Guardian и The Washington Post секретную информацию АНБ, касающуюся тотальной слежки американских спецслужб за информационными коммуникациями между гражданами многих государств по всему миру при помощи существующих информационных сетей и сетей связи, включая сведения о проекте PRISM, а также X-Keyscore и Tempora. По данным закрытого доклада Пентагона, Сноуден похитил 1,7 млн секретных файлов, большинство документов касается «жизненно важных операций американской армии, флота, морской пехоты и военно-воздушных сил». В связи с этим, в США 14 июня 2013 года Сноудену заочно были предъявлены обвинения в шпионаже и похищении государственной собственности, вследствие чего 16 июня Эдвард был объявлен американскими властями в международный розыск. Вскоре Сноуден бежал из США вначале в Гонконг, затем в Россию, где пробыл больше месяца в	ОПК-5

	транзитной зоне аэропорта «Шереметьево». 1 августа 2013 года получил временное убежище в РФ, год спустя — трёхлетний вид на жительство, который в 2017 году продлён до 2020 года. Проживает в России, однако его точное местонахождение не разглашается по соображениям безопасности. Разоблачения Сноудена вызвали жаркие споры о допустимости массового негласного наблюдения, пределах государственной тайны и балансе между защитой персональных данных и обеспечением национальной безопасности в эпоху после 11 сентября 2001 года. Сам Эдвард Сноуден таким образом прокомментировал свои действия: «Я готов пожертвовать всем этим, потому что не могу со спокойной совестью позволить правительству США нарушать приватность, свободу Интернета и основные свободы людей во всём мире с помощью этой громадной системы слежки, которую они втайне разрабатывают», тем самым отсылая нас к международному судебному процессу над бывшими руководителями гитлеровской Германии - Нюрнбергского Трибунала, одним из важнейших положений которого является: «Каждый человек имеет обязательства перед международным сообществом, которые выше обязанности подчиняться местным законам. Следовательно, граждане должны нарушать внутренние законы страны для того, чтобы предотвратить преступления против мира и человечности.» *Проанализируйте данный казус с позиции теоретических основ информационного права и дайте свою правовую оценку действиям Эдварда Сноудена.* *Проведите разграничение частных и публичных интересов (доступ и ограничение доступа к информации).*	

2. Критерии оценивания:

Критерии	Баллы
Задача не решена	0
Задача практически решена с более чем с двумя ошибками	5
Задача практически решена с двумя ошибками	10
Задача решена с одной ошибкой	15
Задача решена без ошибок	20

3. Инструкция и/или методические рекомендации по выполнению

Для решения любой из разноуровневых задач необходимо глубоко изучить соответствующий лекционный материал.

В начале непосредственного решения определённой задачи следует внимательно ознакомиться и формально записать её математическую постановку по принятой форме (дано, найти, путь решения).

Затем целесообразно определить и выписать (из учебного пособия, конспекта лекции, нормативного правового акта) основные нормы для решаемой задачи.

Следующие шаги: осмысление способа и пути решения задачи, вывод (в общем виде) на основе использования известных норм выражения для искомого результата. При этом желательно максимально упростить полученное выражение, используя элементарные юридические знания.

В задачах возможно представление графической иллюстрации решения, которая также позволяет охарактеризовать как результат, так и путь решения задачи.

Темы рефератов (эссе, докладов, сообщений)

1. Перечень компетенций (части компетенции), проверяемых оценочным средством (наименование, код):

   ОПК 5: способность применять нормы материального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.
2. Перечень тем рефератов (эссе, докладов, сообщений):

№ п/п	Тема	Код компетенции
1	Общая характеристика основных источников права информационной безопасности	ОПК-5
2	Правовые гарантии доступа к судебной информации	ОПК-5
3	Понятие и признаки электронного документа	ОПК-5
4	Понятия и юридические свойства электронной подписи	ОПК-5
5	Проблемы применения электронной подписи в Российской Федерации	ОПК-5
6	Цели государства в области обеспечения информационной безопасности	ОПК-5
7	Способы и механизмы совершения информационных компьютерных преступлений	ОПК-5
8	Юридическое понятие тайны. Классификация и правовая характеристика видов тайн	ОПК-5
9	Охрана коммерческой тайны в трудовых отношениях	ОПК-5
10	Охрана персональных данных в трудовых отношениях	ОПК-5
11	Правовой статус субъекта персональных данных	ОПК-5
12	Структура системы правового обеспечения информационной безопасности	ОПК-5
13	Компьютерные преступления как угроза экономической безопасности личности,	ОПК-5

	общества и государства	
14	Основные параметры и черты информационной компьютерной преступности в России	ОПК-5
15	Правовые проблемы охраны государственной тайны	ОПК-5
16	Правовые проблемы охраны коммерческой тайны	ОПК-5
17	Правовые проблемы охраны служебной тайны	ОПК-5
18	Правовые проблемы охраны банковской тайны	ОПК-5
19	Правовые проблемы охраны персональных данных	ОПК-5
20	Правовое регулирование в сфере электронного документооборота	ОПК-5
21	Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя	ОПК-5
22	Ответственность за правонарушения в сфере массовой информации	ОПК-5
23	Правовой режим Интернет-сайта	ОПК-5
24	Правовые проблемы в сфере доменных имен	ОПК-5
25	Основные угрозы компьютерной безопасности при работе в сети Интернет	ОПК-5
26	Саморегулирование в сфере Интернет: опыт России и зарубежных стран	ОПК-5
27	Право граждан на информацию о деятельности органов государственной власти и управления	ОПК-5
28	Правовые режимы информации ограниченного доступа	ОПК-5
29	Международное законодательство в области защиты информации	ОПК-5
30	Правовые вопросы обеспечения информационной безопасности	ОПК-5
31	Ответственность за правонарушения в информационной сфере	ОПК-5
32	Правовое регулирование в области создания и использования информационно-	ОПК-5

	компьютерных технологий	
33	Правовой режим документированной информации	ОПК-5
34	Информационные правоотношения как особый род общественных правоотношений	ОПК-5
35	Правовое регулирование в области создания и использования информационных систем	ОПК-5
36	Правовые проблемы использования информационно-компьютерных технологий в экономике	ОПК-5
37	Правовое регулирование в области использования персональных данных	ОПК-5
38	Правовые проблемы в сфере ГТС Интернет	ОПК-5
39	Юридические фикции в информационном праве и законодательстве	ОПК-5

3. Критерии оценивания:

Критерии	**Баллы**
Тема не раскрыта и/или оформление не соответствует требованиям ФОС.	0
Тема раскрыта недостаточно полно (отсутствуют творческие выводы).	3
Тема раскрыта, творческие выводы сделаны, но имеются погрешности в оформлении.	5
Тема раскрыта, творческие выводы сделаны, оформление соответствует требованиям Университета.	7
Тема раскрыта, творческие выводы сделаны, оформление соответствует требованиям Университета, имеется компьютерная презентация (3 – 5 слайдов).	10

4. Методические рекомендации по написанию

Рефераты (доклады, сообщений) должны быть выполнены на компьютере, оформлены в соответствии с методическими рекомендациями по оформлению письменных работ и в *обязательном* порядке должны содержать титульный лист, рубрики: содержание (оглавление), введение, основную часть, заключение (***творческие*** выводы), список литературы

(включая обязательно литературу кафедры и академии согласно УМК по учебной дисциплине), содержащий не менее трёх наименований со *ссылками* в тексте). Объём реферата: от 10 до 15 страниц машинописного текста (1800 знаков на странице, гарнитура *Times New Roman*).

На все литературные источники (*учебная, научная и специальная* литература) в тексте реферата (статьи) должны быть ссылки в виде: [*N*], где *N* – номер источника в библиографии (списке литературы). На все иные источники (публицистическая, правовая, справочная, энциклопедическая и др. литература; интернет-ресурсы) – сквозные сноски внизу страниц.

Список использованной учебной, научной и специальной литературы должен соответствовать требованиям ГОСТ 7.1–2003 – «Библиографическое описание».

Студент в *обязательном порядке* должен изучить и включить в библиографию (в список литературы) соответствующую теме реферата научную и учебно-методическую литературу кафедры (включая преподавателя, ведущего учебные занятия) и академии, начиная с Рабочей программы учебной дисциплины:

1. Информационное право: учебник/П.У. Кузнецов. – Москва: Юстиция, 2017. - 335с.

2. Информационное право: учебник/ О.А. Городов. - 2-е издание.- Москва: Проспект, 2016.-303 с.

Вспомогательную литературу включать в библиографию в соответствии с рекомендованным в Приложении к рабочей программе № 1 списком научной и учебно-методической литературы.

Тестовые задания

Содержание банка тестовых заданий

V1: {Информационное право}
V2: {Раздел 1. Теоретические основы информационного права.}
V3: {**ОПК 5: способность применять нормы материального права в точном соответствии с правовыми принципами и действующими нормативными правовыми актами с учётом специфики отдельных отраслей права.}**

I: 1
S: Основные принципы вхождения государств в информационное общество провозглашены в:
-: Федеральном законе «Об информации, информационных технологиях и о защите информации»;
+: Окинавской Хартии Глобального Информационного Общества;
-: Федеральном законе «О средствах массовой информации»;
-: Доктрине информационной безопасности Российской Федерации

I: 2
S: Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в:
-: Конституции РФ;
-: Гражданском Кодексе РФ;
+: Доктрине информационной безопасности РФ;
-: Федеральном законе «Об информации, информационных технологиях и о защите информации»

I: 3
S: К государственной тайне не относятся сведения, защищаемые государством …, распространение которых может нанести ущерб государству:
-: в экономической области;
+: в контрразведывательной деятельности;
+: в оперативно-розыскной деятельности;
-: о частной жизни политических деятелей

I: 4
S: Информационная безопасность - это:
-: состояние защищенности информации, циркулирующей в обществе;
-: состояние правовой защищенности информационных ресурсов, информационных продуктов, информационных услуг;
+: 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;
-: состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

I: 5
S: Федеральный закон «О персональных данных» от 27 июля 2006 г. не регулирует отношения, возникающие при:
-: обработке персональных данных, отнесенных к государственной тайне;
+: включении в Единый государственный реестр индивидуальных предпринимателей;
-: обработке персональных данных, отнесенных к служебной тайне.

I: 6
S: С точки зрения информационного права информация – это …
-: сведения о законодательстве, правовых явлениях, правоприменительной деятельности;
-: данные о развитии конкретной правовой науки и ее практическом применении;
+: сведения независимо от формы их представления;
-: форма выражения объективных знаний

I: 7
S: Ответственность за создание вредоносной программы наступает в:
-: любом случае;
+: совокупности с ответственностью за ее использование;
-: случаях, установленных законодательством

Форма тестового задания <u>для зачета и дифференцированного зачета</u> в дистанционном формате

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»

V1: {Информационное право}
V2: {ОПК-5}
F1: {ЗНАТЬ: теорию материального права, принципы и нормы отдельных отраслей материального права. УМЕТЬ: применять принципы и нормы отдельных отраслей материального права. ВЛАДЕТЬ: навыками применения

принципы и нормы отдельных отраслей материального права.}

I:
S: Основные принципы вхождения государств в информационное общество провозглашены в:
-: Федеральном законе «Об информации, информационных технологиях и о защите информации»;
+: Окинавской Хартии Глобального Информационного Общества;
-: Федеральном законе «О средствах массовой информации»;
-: Доктрине информационной безопасности Российской Федерации

I:
S: Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в:
-: Конституции РФ;
-: Гражданском Кодексе РФ;
+: Доктрине информационной безопасности РФ;
-: Федеральном законе «Об информации, информационных технологиях и о защите информации»

I:
S: Предмет информационного права на современном этапе развития законодательства – это …
+: информационные отношения, возникающие в процессе производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации
-: совокупность результатов труда, воплощенных в информации, информационных ресурсов, информационных технологий, средств и технологий коммуникации информации по сетям связи
-: продукты, производные от информации и деятельность, связанная с ними
-: общественные отношения в информационной сфере

I:
S: Не является принципом информационного права:
+: принцип имущественной ответственности;
-: принцип оборотоспособности;
-: принцип распространяемости

I:
S: Впишите пропущенное слово:
… тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности,

распространение которых может нанести ущерб безопасности Российской Федерации:
-: банковская
+: государственная
-: коммерческая

Форма вопросов для зачета (экзамена)

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»

Вопросы, выносимые на зачет, по дисциплине

«Право информационной безопасности»

(наименование дисциплины)

1. Концептуально-логическая модель инфосферы. (инфраструктура, среда, пространство). Проблема информационной безопасности в инфосфере.
2. Определение и содержание понятия «информационная среда» правовой эргасистемы (государства). Взаимосвязь с «информационным пространством».
3. Определение, содержание и различие понятий «информационные процессы» и «информационные технологии». Нетрадиционные (скрытые) информационные каналы.
4. Определение и формализация понятий «ценность информации», «принцип информационной ценности» в эргасистеме.
5. Определение и содержание понятий «качество информации», «количество информации», «единица измерения количества информации».
6. Определение и классификация информации (виды, атрибуты, качественные виды и формы проявления) в эргасистеме.
7. Определение и декомпозиция понятия «защищённость информации» (достоверность, конфиденциальность, сохранность).
8. Определение и декомпозиция понятия «легитимность информации» (аутентичность, легальность, верифицируемость).
9. Классификация и характеристика информационных процессов и информационно-правовых режимов в инфосфере.
10. Классификация поколений информационных технологий, «информационные революции». Новая информационная технология (принцип «автоформализации»).
11. Классификация основных информационных отношений в инфосфере. Информационная борьба (война).
12. Информационное общество и право, информационно-правовое знание. Окинавская Хартия. Роль информационного права в обеспечении национальной безопасности. Основные задачи государственной информационной политики РФ.
13. Понятие, признаки и классификация (виды) информации.
14. Общие (актуальность и защищённость) и специальные (легитимность) свойства информации, принципиальные для правового регулирования информационных отношений.

15. Классификация, общая характеристика и субъектно-объектный состав информационных правоотношений.

16. Характеристика права на поиск, получение и использование информации.

17. Документированная информация как объект информационных правоотношений. Конституционные основы и правовой режим документированной информации.

18. Правовой режим информационных систем, информационных технологий и средств их обеспечения. Государственная политика в области их создания.

19. Правовое регулирование отношений в области связи, телекоммуникаций и автоматизированных систем (типа ГАС РФ «Правосудие», ГАС РФ «Выборы», ГАС РФ «Управление»).

20. Правовые проблемы информационной безопасности личности, общества и государства. Информационная безопасность абонента ГТС Интернет.

21. Модель информационной безопасности судебных автоматизированных систем: правовое регулирование и юрисдикция.

22. Правовые проблемы использования глобальной информационно-вычислительной ГТС Интернет (доменные имена и товарные знаки). Особенности правового регулирования информационных отношений.

23. Право информационной безопасности как наука и учебная дисциплина.

24. Правовой режим глобальной информационно-вычислительной сети Интернет. Проблема ответственности за размещение информации компрометирующего характера в ГТС Интернет.

25. Проблемы и способы международно-правового обеспечения глобального информационного обмена.

26. Правовые режимы информации.

27. Понятие и классификация «информационного оружия». Угрозы его применения.

28. Понятие информационного законодательства и его система.

29. Особенности правового регулирования информационных отношений в области массовой информации в Российской Федерации.

30. Институт тайны как способ правовой защиты информации ограниченного доступа.

31. Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации».

32. Проблемы правового регулирования информационных отношений в области коммерческой тайны.

33. Особенности правового регулирования информационных отношений в области персональных данных. Обязанности оператора персональных данных.

34. Правовое регулирование применения квалифицированной (электронно) подписи в России. Правовые свойства (аутентичность, легальность, верифицируемость) информации.

35. Правовая информатизация как объективный социально-экономический процесс. Проблемы создания и архитектура ГАС РФ «Правосудие».

36. Проблема и способы правового сдерживания информационно-компьютерной преступности в России.

37. Особенности неправомерного доступа к «компьютерной» информации. Трудности юридической квалификации и пути их преодоления.

38. Особенности и модели правового регулирования применения электронной подписи за рубежом.

39. Особенности правового регулирования доступа к статистической информации о деятельности судов.

40. Особенности квалификации и расследования преступлений в сфере компьютерной информации.

41. Проблемы и морально-правовые аспекты тайны усыновления. Усыновление как юридическая фикция.

42. Информационные аспекты формирования правосознания.

43. Принципы создания единой правовой нормативно-методической базы автоматизированных систем судопроизводства. Классификация судебной информации.

44. Структура и общая характеристика информационного законодательства.

45. Особенности правового регулирования информационных отношений в области государственной тайны.

46. Информационные аспекты интеллектуальной собственности. Особенности правового регулирования информационных отношений институтом патентного права.

47. Концепция информационного законодательства в РФ.

48. Понятие и виды ответственности за правонарушения в информационной сфере.

49. Доктрина информационной безопасности РФ об основных угрозах в информационной сфере и их источниках.

50. Понятие государственной тайны и критерии охраноспособности прав на нее. Объект и субъекты права на государственную тайну.

ПЕРЕЧЕНЬ ДОПОЛНИТЕЛЬНЫХ ВОПРОСОВ

1. Конституционные принципы обеспечения информационной безопасности (ст. 24; 29; 42; 43, п. 1; ст. 44, п. 1, 2).

2. АПК РФ от 24.07.02: Статья 75, п. 1, 3 (ЭЦП): характеристика информационно-правовой нормы.

3. ГК РФ, ч. 1 от 30.11.94 г.: ст. 139 (служебная и коммерческая тайна) – характеристика информационно-правового режима.

4. ГК РФ, ч. 1 от 30.11.94 г.: ст. 150 (личная и семейная тайна) – характеристика информационно-правового режима.

5.ГК РФ, ч. 1 от 30.11.94 г.: ст. 857 (банковская тайна) – характеристика информационно-правового режима.

6. ГК РФ, ч. 1 от 30.11.94 г.: ст. 1123 (тайна завещания) – характеристика информационно-правового режима.

7. КоАП РФ от 30.12.01: статья 13.14 (служебная или профессиональная тайна) – характеристика информационно-правового режима.

8. КоАП РФ от 30.12.01: статья 13.15 («скрытые вставки») – характеристика информационно-правовой нормы.

9. УК РФ от 13.06.96: статья 183 (коммерческая, налоговая или банковская тайна) – характеристика информационно-правового режима.

10. УК РФ от 13.06.96: статья 138 (тайна связи) – характеристика информационно-правового режима.

11. УК РФ от 13.06.96: статьи 272, 273, 274 (доступ к информации) – характеристика информационно-правовых норм.

12. УК РФ от 13.06.96: статьи 283, 284 (государственная тайна) – характеристика информационно-правового режима.

13. УК РФ от 13.06.96: 310 (тайна следствия), 311(тайна судопроизводства) – характеристика информационно-правовых режимов.

14. УК РФ от 13.06.96: статья 140 (отказ в информации) – характеристика информационно-правового режима.

15. УК РФ от 13.06.96: статья 141 (тайна голосования) – характеристика информационно-правового режима.

16. УК РФ от 13.06.96: статья 137 (личная или семейная тайна) – характеристика информационно-правового режима.

17. УК РФ от 13.06.96: статья 155 (тайна усыновления/удочерения) – характеристика информационно-правового режима.

18. ФЗ от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: Статья 11: юридическая сила электронного документа с учётом ФЗ от 06.04.11 № 63-ФЗ (замена ЭЦП).

19. ФЗ от 06.04.11 № 63-ФЗ «Об электронной подписи»: условия юридической силы ЭП; юридические свойства ЭЦП; условия равнозначности электронного документа и документа на бумажном носителе.

20. ГОСТ Р ИСО/МЭК 15408-3-2002. Скрытые каналы (понятие, требования к анализу).

21. Законодательная база применения электронной подписи (ГК РФ, ФЗ об информации, ФЗ об ЭП).

Заведующий кафедрой _____/ _____
(подпись) (ФИО)

Критерии оценивания зачета:

Критерии	Баллы
ДКЗ выполнено и/или классная контрольная летучка выполнена с оценкой «удовлетворительно»	21-40
ДКЗ не выполнено или выполнено с оценкой «неудовлетворительно» и/или классная контрольная летучка выполнена с оценкой «неудовлетворительно»	0-20
На теоретический вопрос дан полный ответ, на теоретико-прикладной вопрос дан неполный ответ и в решении практической задачи допущено не более одной ошибки (16 – 60 баллов).	37-100
На теоретический и на теоретико-прикладной вопросы ответы не даны и/или практическая задача не решена (0 – 15 баллов).	0-36

Форма контрольного задания (промежуточной аттестации)

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРАВОСУДИЯ»

Образовательная программа _40.05.03_Судебная экспертиза_____
(код и наименование программы)
Дисциплина _____Право информационной безопасности_____
(наименование дисциплины)

БИЛЕТ № 1
(Образец)

1. Роль права информационной безопасности в обеспечении национальной безопасности. Основные задачи государственной политики в сфере информационной безопасности РФ.
2. Характеристика права на поиск, получение и использование информации.
3. Задача…….

Заведующий кафедрой _____ / _____
(подпись) (ФИО)

Критерии оценивания *контрольного задания (промежуточной аттестации)*

Критерии	**Баллы**
На теоретический вопрос дан полный ответ, на теоретико-прикладной вопрос дан неполный ответ и в решении практической задачи допущено не более одной ошибки (16 – 60 баллов).	37-100
На теоретический и на теоретико-прикладной вопросы ответы не даны и/или практическая задача не решена (0 – 15 баллов).	0-36