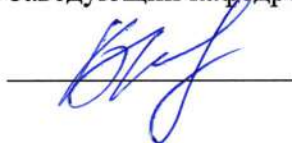


**Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»
Кафедра юриспруденции**

УТВЕРЖДЕН
на заседании кафедры
«19» мая 2025 г., протокол № 6
Заведующий кафедрой информатики



Бреднева В.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.О.08 «Основы IT права»

Направление подготовки
09.03.03 Прикладная информатика

профиль

Автоматизированные системы обработки информации и управления

**Уровень высшего образования
БАКАЛАВРИАТ**

Южно-Сахалинск,
2025 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность. УК-2.2. Умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты решений для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности. УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта, навыками работы с нормативно-правовой документацией.
УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1 Знать задачи и направления государственной политики в сфере противодействия коррупции. УК-10.2 Уметь определять содержание полномочий государственных органов в сфере противодействия коррупции, объяснять отрицательное влияние коррупции на общество и воспитывать нетерпимость к коррупции УК-10.3 Иметь необходимые навыки в сфере противодействия коррупции

2. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Предмет, метод, система и принципы информационного права	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету
2.	Источники информационного права. Система	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к

	законодательства в информационной сфере. Нормы информационного права		зачету
3.	Правоотношения в информационной сфере	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету
4.	Правовой режим информации. Право на информацию. Охрана и защита права на информацию	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету
5.	Правовые основы обеспечения информационной безопасности	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету
6.	Институт государственной тайны	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету
7.	Институт коммерческой тайны	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету
8.	Институт персональных данных	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету
9.	Правовое регулирование в области оборота документированной информации. Электронный документооборот. Электронная цифровая подпись	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету
10.	Правовое регулирование в области создания и использования автоматизированных информационных систем	УК-2; УК-10	Задания к практическим работам, контрольные вопросы, вопросы к зачету

3. Оценочные средства

Тестирование является одним из средств формального контроля качества обучения – методе, основанном на стандартизированных заданиях, которые позволяют оценить знания, умения и навыки испытуемого

Требования к составлению тестового задания

Тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

– **закрытая** форма – является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя один или несколько правильных ответов.

Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде.

Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

– **открытая** форма – вопрос представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие – части слова или буквы, условные обозначения, линии или изображения элементов схемы или графика.

Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

– **установление соответствия** – в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

– **установление последовательности** – предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз

Примерный тест

Задания для проверки сформированности компетенции:

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-10 Способен формировать нетерпимое отношение к коррупционному поведению

ЧАСТЬ 1. МНОЖЕСТВЕННЫЙ ВЫБОР (5 вопросов, 1 балл = 5 баллов)

Вопрос 1.

Какой нормативный правовой акт является базовым в сфере регулирования информационных отношений в Российской Федерации?

А. Гражданский кодекс РФ

Б. Федеральный закон «Об информации, информационных технологиях и о защите информации»

В. Конституция РФ

Г. Федеральный закон «О персональных данных»

✓ **Ответ: Б. Федеральный закон «Об информации, информационных технологиях и о защите информации»**

Пояснение: Этот закон (№ 149-ФЗ) определяет основные понятия и принципы правового регулирования в информационной сфере.

Вопрос 2.

Что из перечисленного НЕ относится к основным признакам информации как объекта правовых отношений?

А. Нематериальность

Б. Ограниченность в пространстве

В. Возможность неограниченного тиражирования

Г. Исчерпаемость

✓ **Ответ: Б. Ограниченность в пространстве**

Пояснение: Информация не имеет физических границ, она может одновременно находиться в разных местах.

Вопрос 3.

Какой вид тайны относится к сведениям, защищаемым государством в области его военной, внешнеполитической, экономической, разведывательной и контрразведывательной деятельности?

- А. Коммерческая тайна
- Б. Служебная тайна
- В. Государственная тайна
- Г. Профессиональная тайна

✓ **Ответ: В. Государственная тайна**

Пояснение: Определение дано в Законе РФ «О государственной тайне».

Вопрос 4.

Какая информация НЕ может быть отнесена к коммерческой тайне?

- А. Сведения о задолженности работников по заработной плате
- Б. Результаты интеллектуальной деятельности
- В. Сведения о применяемых технологиях
- Г. Информация о проведении переговоров

✓ **Ответ: А. Сведения о задолженности работников по заработной плате**

Пояснение: Ст. 5 Федерального закона «О коммерческой тайне» устанавливает перечень сведений, которые не могут составлять коммерческую тайну, включая задолженность по зарплате.

Вопрос 5.

Что понимается под электронной цифровой подписью (ЭЦП) в российском законодательстве?

- А. Графическое изображение подписи в электронном документе
- Б. Информация в электронной форме, присоединяемая к подписываемому документу и позволяющая идентифицировать владельца сертификата ключа подписи
- В. Скан-копия собственноручной подписи
- Г. Пароль доступа к электронному документу

✓ **Ответ: Б. Информация в электронной форме, присоединяемая к подписываемому документу и позволяющая идентифицировать владельца сертификата ключа подписи**

Пояснение: Определение дано в Федеральном законе «Об электронной подписи».

ЧАСТЬ 2. ЧИСЛОВОЙ ОТВЕТ (4 вопроса, 2 балла = 8 баллов)**Вопрос 6.**

Сколько глав содержит Федеральный закон «Об информации, информационных технологиях и о защите информации» (№ 149-ФЗ) в действующей редакции?

✓ **Ответ: 6**

Пояснение: Закон состоит из 6 глав: общие положения, информационные системы, оборот информации, защита информации, государственное регулирование, заключительные положения.

Вопрос 7.

В каком году была принята действующая Конституция Российской Федерации, закрепившая право на неприкосновенность частной жизни и право на информацию?

✓ **Ответ: 1993**

Пояснение: Конституция РФ принята всенародным голосованием 12 декабря 1993 года.

Вопрос 8.

Какое минимальное количество работников обязательно для введения режима коммерческой тайны в организации?

✓ **Ответ: 1**

Пояснение: Режим коммерческой тайны может быть введен даже при одном работнике (индивидуальный предприниматель или директор — единственный учредитель).

Вопрос 9.

В течение какого срока оператор персональных данных обязан уничтожить персональные данные после достижения цели их обработки (если иное не предусмотрено законом)?

✓ **Ответ: 30 дней**

Пояснение: Ст. 21 Федерального закона «О персональных данных» — 30 дней с момента достижения цели обработки.

ЧАСТЬ 3. УСТАНОВЛЕНИЕ СООТВЕТСТВИЯ (3 вопроса, 2 балла = 6 баллов)

Вопрос 10.

Установите соответствие между видом тайны и нормативным правовым актом, регулирующим её правовой режим:

№	Вид тайны	№	Нормативный правовой акт
1	Государственная тайна	А	Федеральный закон «О коммерческой тайне»

№	Вид тайны	№	Нормативный правовой акт
2	Коммерческая тайна	Б	Федеральный закон «О персональных данных»
3	Персональные данные	В	Федеральный закон «О банках и банковской деятельности»
4	Банковская тайна	Г	Закон РФ «О государственной тайне»

✓ **Ответ:**

1 — Г

2 — А

3 — Б

4 — В

Вопрос 11.

Установите соответствие между принципом информационного права и его содержанием:

№	Принцип	№	Содержание
1	Принцип свободы информации	А	Информация должна создаваться и распространяться свободно, за исключением ограничений, установленных законом
2	Принцип достоверности	Б	Информация должна соответствовать реальному положению дел
3	Принцип своевременности	В	Информация должна предоставляться в установленные сроки
4	Принцип конфиденциальности	Г	Обязательное соблюдение режима ограниченного доступа к определенным категориям сведений

✓ **Ответ:**

1 — А

2 — Б

3 — В

4 — Г

Вопрос 12.

Установите соответствие между субъектом информационных правоотношений и его характеристикой:

№	Субъект	№	Характеристика
1	Обладатель информации	А	Лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации
2	Оператор информационной системы	Б	Гражданин, к которому относятся персональные данные
3	Субъект персональных данных	В	Лицо, осуществляющее деятельность по обработке информации в информационной системе
4	Владелец сайта в сети Интернет	Г	Лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта

✓ **Ответ:**

- 1 — А
- 2 — В
- 3 — Б
- 4 — Г

ЧАСТЬ 4. ОТКРЫТЫЕ ВОПРОСЫ (7 вопросов, 3 балла = 21 балл)

Вопрос 13.

Назовите основные принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации, закрепленные в Федеральном законе «Об информации, информационных технологиях и о защите информации».

✓ **Эталон ответа:**

1. Свобода поиска, получения, передачи, производства и распространения информации любым законным способом.
2. Установление ограничений доступа к информации только федеральными законами.
3. Открытость информации о деятельности государственных органов и органов местного самоуправления.
4. Равноправие языков народов РФ при создании информационных систем и их эксплуатации.
5. Обеспечение безопасности РФ при создании информационных систем и их эксплуатации.
6. Достоверность информации и своевременность её предоставления.
7. Неприкосновенность частной жизни, недопустимость сбора информации о частной жизни без согласия.
8. Недопустимость установления нормативными правовыми актами преимуществ применения одних информационных технологий перед другими.

Вопрос 14.

Раскройте понятие «персональные данные». Какие сведения относятся к специальным категориям персональных данных, и каковы особенности их обработки?

✓ **Эталон ответа:**

Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Специальные категории персональных данных (ст. 10 ФЗ «О персональных данных»):

- расовая, национальная принадлежность;
- политические взгляды;
- религиозные или философские убеждения;
- состояние здоровья;
- интимная жизнь.

Особенности обработки: по общему правилу обработка специальных категорий не допускается. Исключения: наличие письменного согласия субъекта; обработка в целях трудового законодательства; защита жизни и здоровья; медико-профилактические цели; деятельность религиозных организаций и др.

Вопрос 15.

Опишите порядок введения режима коммерческой тайны в организации. Какие меры должен предпринять работодатель?

✓ **Эталон ответа:**

1. Издание приказа (распоряжения) о введении режима коммерческой тайны.
 2. Утверждение перечня сведений, составляющих коммерческую тайну.
 3. Разработка и утверждение Положения о коммерческой тайне.
 4. Ознакомление работников под роспись с перечнем и Положением.
 5. Нанесение на материальные носители грифа «Коммерческая тайна».
 6. Ведение учета лиц, получивших доступ к коммерческой тайне.
 7. Регулирование отношений с контрагентами (включение условий о конфиденциальности в договоры).
-

Вопрос 16.

Что понимается под электронным документооборотом? Какие виды электронных подписей предусмотрены российским законодательством?

✓ **Эталон ответа:**

Электронный документооборот — система создания, обработки, хранения, передачи и использования электронных документов с применением информационных технологий.

Виды электронных подписей (ФЗ «Об электронной подписи»):

1. **Простая электронная подпись** — подтверждает факт формирования электронной подписи определенным лицом с использованием кодов, паролей и иных средств.

2. **Усиленная неквалифицированная электронная подпись** — получена в результате криптографического преобразования информации с использованием ключа электронной подписи; позволяет определить лицо, подписавшее документ, и обнаружить факт внесения изменений.
 3. **Усиленная квалифицированная электронная подпись** — обладает всеми признаками неквалифицированной, но сертификат ключа проверки выдан аккредитованным удостоверяющим центром.
-

Вопрос 17.

Назовите основные угрозы информационной безопасности, выделенные в Доктрине информационной безопасности Российской Федерации.

✓ **Эталон ответа:**

1. Нарастание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру РФ.
 2. Деятельность террористических и экстремистских организаций в информационной сфере.
 3. Использование информационных технологий для вмешательства во внутренние дела РФ.
 4. Увеличение масштабов компьютерной преступности.
 5. Недостаточный уровень развития конкурентоспособных информационных технологий.
 6. Зависимость отечественной промышленности от зарубежных информационных технологий.
 7. Недостаточная эффективность научных исследований в области информационной безопасности.
-

Вопрос 18.

Какие сведения НЕ могут быть отнесены к государственной тайне? Приведите не менее трех категорий.

✓ **Эталон ответа:**

В соответствии со ст. 7 Закона РФ «О государственной тайне», не подлежат отнесению к государственной тайне и засекречиванию сведения:

1. О чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях.
 2. О состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, преступности.
 3. О привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам.
 4. О фактах нарушения прав и свобод человека и гражданина.
 5. О размерах золотого запаса и государственных валютных резервах РФ.
 6. О состоянии здоровья высших должностных лиц РФ.
 7. О фактах нарушения законности органами государственной власти и их должностными лицами.
-

Вопрос 19.

Раскройте содержание права на доступ к информации. Какие ограничения этого права установлены законодательством?

✓ Эталон ответа:

Право на доступ к информации — закрепленная Конституцией РФ (ст. 29) возможность каждого искать, получать, передавать, производить и распространять информацию любым законным способом.

Ограничения права на доступ (ст. 9 ФЗ № 149-ФЗ):

1. Ограничение доступа к информации устанавливается федеральными законами.
 2. Доступ может быть ограничен в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.
 3. Обязательным является соблюдение конфиденциальности информации ограниченного доступа.
 4. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством о государственной тайне.
 5. Запрещается требовать от гражданина предоставления информации о его частной жизни, включая сведения, составляющие личную или семейную тайну, и получать такую информацию помимо воли гражданина.
-

Вопрос 20.

Какие меры ответственности предусмотрены за разглашение персональных данных? Охарактеризуйте виды юридической ответственности.

✓ Эталон ответа:

За нарушение законодательства о персональных данных предусмотрены следующие виды ответственности:

1. **Дисциплинарная ответственность** (для работников) — замечание, выговор, увольнение (ст. 192 ТК РФ).
2. **Административная ответственность** (ст. 13.11 КоАП РФ):
 - обработка персональных данных без согласия — штраф до 100 000 руб.
 - невыполнение оператором обязанности по опубликованию политики обработки — штраф до 30 000 руб.
 - иные составы.
3. **Уголовная ответственность** (ст. 137 УК РФ):
 - незаконное собирание или распространение сведений о частной жизни лица без его согласия — штраф до 200 000 руб., либо обязательные работы, либо арест.
 - квалифицированные составы (с использованием служебного положения) — штраф до 300 000 руб., либо лишение свободы до 4 лет.
4. **Гражданско-правовая ответственность:**
 - возмещение убытков;
 - компенсация морального вреда.

Критерии оценки знаний при проведении тестирования

Отметка **«отлично»** выставляется при условии правильного ответа не менее чем 85% тестовых заданий;

Отметка **«хорошо»** выставляется при условии правильного ответа не менее чем 70 % тестовых заданий;

Отметка **«удовлетворительно»** выставляется при условии правильного ответа не менее 50 %;

Отметка **«неудовлетворительно»** выставляется при условии правильного ответа менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации