Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Крылова Людмила Вячеславовна
Должность: Проректор по учебно-методической работе
Дата подписания: 07.11.2026 20:11:38
Уникальный программный ключ:
b066544bae1e449cd8bfce392f7224a6f6a27162

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И ТОРГОВЛИ ИМЕНИ МИХАИЛА ТУГАН-БАРАНОВСКОГО»

Кафедра финансов и экономической безопасности

УТВЕРЖДАЮ

Заведующий кафедрой
_____ Омельянович Л.А.
(подпись)

«18» 02 2026 г.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по учебной дисциплине

Б1.О.44. Коммерческая тайна
(шифр и наименование учебной дисциплины)

38.05.01 Экономическая безопасность
(код и наименование специальности)

Экономико-правовое обеспечение экономической безопасности
(наименование специализации)

Разработчик:
доцент _____ Канеева Инара Исмаиловна
(должность) (подпись)

Оценочные материалы рассмотрены и утверждены на заседании кафедры
от «18» 02 2026 г., протокол № 20

Донецк 2026 г.

Паспорт
оценочных материалов по учебной дисциплине (модулю)

Коммерческая тайна

(наименование учебной дисциплины)

Перечень компетенций, формируемых в результате освоения учебной дисциплины (модуля)

№ п/п	Код и наименование контролируемой компетенции	Контролируемые разделы (темы) учебной дисциплины	Этапы формирования (семестр изучения)
1	ОПК-5. Способен осуществлять профессиональную деятельность в соответствии с нормами профессиональной этики, нормами права, нормативными правовыми актами в сфере экономики, исключающими противоправное поведение	Тема 1. Коммерческая тайна как элемент хозяйственной деятельности	8
		Тема 2. Коммерческая тайна как объект правовой защиты	8
		Тема 3. Экономический шпионаж как инструмент конкурентной борьбы	8
		Тема 4. Основы конкурентной разведки: стратегии и методы	8
		Тема 5. Конкурентная контрразведка - деятельность по защите экономических интересов предприятия	8
		Тема 6. Способы охраны коммерческой тайны предприятия	8

ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Таблица 2 - Показатели оценивания компетенций

№ п/п	Код контролируемой компетенции	Код и наименование индикатора достижения компетенции	Контролируемые разделы (темы) учебной дисциплины	Наименование оценочного средства
1	ОПК-5. Способен осуществлять профессиональную деятельность в соответствии с нормами профессиональной этики, нормами права, нормативными правовыми актами в сфере экономики, исключающими противоправное поведение	ИДК 1 - Способен выполнять профессиональные задачи в соответствии с нормами профессиональной этики и нормами права	Тема 1. Коммерческая тайна как элемент хозяйственной деятельности	Тест, собеседование (устный опрос), доклад
			Тема 2. Коммерческая тайна как объект правовой защиты	Тест, собеседование (устный опрос), доклад, контрольная работа (ТМК1)
			Тема 3. Экономический шпионаж как инструмент конкурентной борьбы	Тест, собеседование (устный опрос), доклад
			Тема 4. Основы конкурентной разведки: стратегии и методы	Тест, собеседование (устный), доклад, контрольная работа (ТМК2)
		ИДК 2 - Способен соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в сфере экономики, исключающими противоправное поведение	Тема 5. Конкурентная контрразведка - деятельность по защите экономических интересов предприятия	Тест, собеседование (устный опрос), доклад
			Тема 6. Способы охраны коммерческой тайны предприятия	Тест, собеседование (устный), доклад, контрольная работа (ТМК3)

Таблица 3 - Критерии и шкала оценивания по оценочному материалу «Тест»

Шкала оценивания (интервал баллов)	Критерии оценивания
4-5	Процент правильных ответов составляет 90-100%
2-3	Процент правильных ответов составляет 51-89%
0-1	Процент правильных ответов составляет 0-50%

Таблица 4 - Критеии и шкала оценивания по оценочному материалу «Собеседование (устный опрос)»

Шкала оценивания (интервал баллов)	Критерии оценивания
4-5	Ответы на вопросы представлены на высоком уровне (обучающийся полно осветил рассматриваемую проблематику, привел аргументы в

	пользу своих суждений, владеет профильным понятийным аппаратом)
2-3	Ответы на вопросы представлены на среднем уровне (обучающийся в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности)
0-1	Ответы на вопросы представлены на неудовлетворительном уровне или не представлен (обучающийся не готов, не выполнил задание и т.п.)

Таблица 5 - Критерии и шкала оценивания по оценочному материалу «Доклад»

Шкала оценивания (интервал баллов)	Критерии оценивания
3-4	Доклад представлен на высоком уровне (обучающийся полно осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным аппаратом)
1-2	Доклад представлен на среднем уровне (обучающийся в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности)
0-0,5	Доклад представлен на неудовлетворительном уровне или не представлен (обучающийся не готов, не выполнил задание и т.п.)

Таблица 6 - Критерии и шкала оценивания по оценочному материалу «Контрольная работа» (ТМК)

Шкала оценивания (интервал баллов)	Критерии оценивания
7-8	Контрольная работа выполнена на высоком уровне (правильные ответы даны на 90-100% вопросов/задач)
5-6	Контрольная работа выполнена на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3-4	Контрольная работа выполнена на низком уровне (правильные ответы даны на 36-74% вопросов/задач)
0-2	Контрольная работа не выполнена или выполнена на неудовлетворительном уровне (правильные ответы даны менее 35% вопросов/задач)

Таблица 7 - Перечень оценочных материалов по учебной дисциплине «Коммерческая тайна»

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	Собеседование (устный опрос)	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой учебной дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по учебной дисциплине или определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам учебной дисциплины
2	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий

3	Доклад	Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно- исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Тематика докладов
4	Контрольная работа (ТМК)	Средство проверки умений применять полученные знания для решения задач определенного типа по теме, разделу или учебной дисциплине.	Комплект контрольных заданий по вариантам

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ

Методические материалы отражают основные сведения о каждом оценочном средстве, используемом в ходе изучения учебной дисциплины «Коммерческая тайна» для контроля результатов обучения.

При изучении учебной дисциплины в течение семестра обучающийся максимально может набрать 100 баллов.

Текущий контроль знаний обучающихся осуществляется на основании оценки систематичности и активности по каждой теме программного материала учебной дисциплины.

Текущий контроль знаний обучающихся осуществляется с помощью тестов, докладов, собеседования, контрольных работ.

Собеседование (устный опрос) осуществляется по лекционному материалу и материалу для самостоятельного изучения обучающимся. Развернутый ответ обучающегося должен представлять собой связное, логически последовательное сообщение на заданную тему, показывать его умение применять определения, правила в конкретных случаях.

Тестирование по темам смысловых модулей может проводиться в компьютерных классах с помощью программы «Тесты» согласно графика проведения модульного контроля.

Опираясь на знания обучающихся, преподаватель оставляет за собой право решающего слова во время оценивания знаний.

Система оценивания всех видов работ по учебной дисциплине приведена в таблице 8.

Таблица 8 – Система начисления баллов по текущему контролю знаний

Максимально возможный балл по виду учебной работы					
Смысловые модули	Текущая аттестация				Итого
	Собеседование (устный опрос)	Доклад	Тест	Контрольная работа	
Смысловой модуль 1. Теоретические подходы и правовые основы защиты коммерческой тайны предприятия	10	6	10	8	34
Смысловой модуль 2. Разведка на предприятии	10	4	10	8	32
Смысловой модуль 3 Конкурентная контрразведка: механизм противодействия утечке информации	10	6	10	8	34
Итого:	30	16	30	24	100

Промежуточная аттестация осуществляется в форме зачета. Опираясь на знания обучающихся, преподаватель оставляет за собой право решающего слова во время оценивания знаний.

Таблица 9 - Распределение баллов, которые получают обучающиеся

Максимальное количество баллов за текущий контроль и самостоятельную работу						**Максимальная сумма баллов**
Смысловой модуль 1		**Смысловой модуль 2**		**Смысловой модуль 3**		100
Т1	Т2	Т3	Т4	Т5	Т6	
16	16	17	17	17	17	

Примечание. Т1, Т2, ... Т6 – номера тем соответствующих смысловых модулей

Таблица 10 - Соответствие государственной шкалы оценивания академической успеваемости

Сумма баллов за все виды учебной деятельности	**По государственной шкале**	**Определение**
90-100	5 «отлично» / зачтено	отличное выполнение с незначительным количеством неточностей
75-89	4 «хорошо» / зачтено	в целом правильно выполненная работа с незначительным количеством ошибок
60-74	3 «удовлетворительно» / зачтено	удовлетворительное выполнение со значительным количеством недостатков
менее 60	2 «неудовлетворительно» / не зачтено	с возможностью повторной аттестации

Примеры типовых контрольных заданий

Вопросы для собеседования (устного опроса)

Смысловой модуль 1. Теоретические подходы и правовые основы защиты коммерческой тайны предприятия

Тема 1. Коммерческая тайна как элемент хозяйственной деятельности

1. Приведите классификацию информации по режиму доступа к ней.
2. Раскройте сущность и значение коммерческой тайны в условиях взаимодействия конкурирующих предприятий
3. Дайте определение понятию «коммерческая тайна».
4. Назовите подходы к определению и соотношению с понятиями «ноу-хау» (know how) и «торговый секрет» (trade secret), «служебная тайна» и «профессиональная тайна».
5. Соотнесите понятия «коммерческая тайна» и «интеллектуальная собственность».
6. Определите предмет коммерческой тайны.
7. Раскройте признаки коммерческой тайны.

Тема 2. Коммерческая тайна как объект правовой защиты

1. Назовите правовые основы функционирования института коммерческой тайны.
2. Коммерческая тайна в законодательстве зарубежных стран и в международном праве.
3. Определите субъекты коммерческой тайны.
4. Раскройте имущественные права интеллектуальной собственности на коммерческую тайну.
5. Охарактеризуйте стратегию охраны коммерческой тайны.
6. Раскройте понятие «режим коммерческой тайны».
7. Дате определение понятий «патентное право» и «авторское» право.
8. Назовите виды правовой ответственности за нарушение режима коммерческой тайны.

Смысловой модуль 2. Разведка на предприятии

Тема 3. Экономический шпионаж как инструмент конкурентной борьбы

1. Раскройте понятие и сущность экономического шпионажа как инструмента конкуренции.
2. Охарактеризуйте признаки экономического шпионажа.
3. Раскройте историю экономического шпионажа.
4. Назовите технические методы экономического шпионажа.
5. Охарактеризуйте агентурные методы экономического шпионажа.
6. Назовите этические аспекты экономического шпионажа.

Тема 4. Основы конкурентной разведки: стратегии и методы

1. Конкурентная разведка: понятие, задачи, принципы.
2. Назовите основные признаки конкурентной разведки.
3. Охарактеризуйте виды конкурентной разведки.
4. Определите стратегии конкурентной разведки.
5. Охарактеризуйте методы конкурентной разведки.

6. Служба конкурентной разведки предприятия: организация, функции.

Смысловой модуль 3. Конкурентная контрразведка: механизм противодействия утечке информации

Тема 5. Конкурентная контрразведка - деятельность по защите экономических интересов предприятия

1. Раскройте сущность и основные направления конкурентной контрразведки.
2. Укажите уровни и виды конкурентной контрразведки.
3. Назовите информационные войны и их виды.
4. Черный PR: защита и нападение в бизнесе.

Тема 6. Способы охраны коммерческой тайны предприятия

1. Назовите основные направления и виды охраны коммерческой тайны.
2. Охарактеризуйте правовые меры охраны коммерческой тайны.
3. Определите охрану коммерческой тайны в рамках отношений «работодатель-работник».
4. Охрана коммерческой тайны от третьих лиц.
5. Охрана коммерческой тайны в отношениях с государством.
6. Охрана коммерческой тайны от конкурентов.
7. Назовите организационные меры охраны коммерческой тайны.
8. Охарактеризуйте технические меры охраны коммерческой тайны.
9. Назовите психологические меры охраны коммерческой тайны. Приведите пример.

Темы докладов:

Смысловой модуль 1. Теоретические подходы и правовые основы защиты коммерческой тайны предприятия

Тема 1. Коммерческая тайна как элемент хозяйственной деятельности

1. Понятие и роль информации в жизни современного общества.
2. Гарантии информационных прав граждан.
3. Права граждан в информационной сфере.
4. Информационные войны: проблемы правового регулирования.

Тема 2. Коммерческая тайна как объект правовой защиты

1. Ключевые проблемы информационной безопасности государства.
2. Принципы государственной политики обеспечения информационной безопасности.
3. Состояние и эффективность законодательства о коммерческой тайне.
4. Основные обязанности органов законодательной власти в сфере информационной безопасности.
5. Основные обязанности органов исполнительной власти в сфере информационной безопасности.
6. Основные обязанности органов судебной власти в сфере информационной безопасности.

Смысловой модуль 2. Разведка на предприятии

Тема 3. Экономический шпионаж как инструмент конкурентной борьбы

1. Понятие и сущность экономического шпионажа инструмента конкуренции.
2. Особенности экономического и промышленного шпионажа.
3. Историческое развитие экономического шпионажа.
4. Характерные особенности конкурентной разведки и экономического шпионажа.
5. Агентурные методы экономического шпионажа.
6. Технические методы экономического шпионажа
7. Этические аспекты экономического шпионажа.
8. Опыт работы службы конкурентной разведки западными фирмами.

Тема 4. Основы конкурентной разведки: стратегии и методы

1. Понятие, задачи и принципы конкурентная разведки.
2. Основные признаки конкурентной разведки.
3. Виды конкурентной разведки.
4. Основные стратегии конкурентной разведки.
5. Современные методы конкурентной разведки.
6. Организация и функции службы конкурентной разведки предприятия.

Смысловой модуль 3 Конкурентная контрразведка: механизм противодействия утечке информации

Тема 5. Конкурентная контрразведка - деятельность по защите экономических интересов предприятия

1. Опыт работы службы конкурентной разведки западными фирмами.
2. Понятийный аппарат конкурентной разведки: соотношение терминов и понятий.
3. Характеристика конкурентной разведки современного предприятия.
4. Стратегии конкурентной разведки: сущность и примеры.
5. Служба конкурентной разведки предприятия: организация, функции.
6. Методы конкурентной разведки.

Тема 6. Способы охраны коммерческой тайны предприятия

1. Договорные отношения в информационной сфере: понятие, виды и условия.
2. Трудовые отношения по поводу использования и защиты коммерчески значимой информации.
3. Понятие и признаки коммерчески значимой информации.
4. Юридическая ответственность лиц, совершивших правонарушения в сфере обращения коммерчески значимой информации.

Варианты типовых тестовых заданий:

1. **Режим защиты информации не устанавливается в отношении сведений, относящихся к:**

а) государственной тайне;
б) деятельности государственных деятелей;
в) конфиденциальной информации;
г) персональным данным.

2. В регистрации средства массовой информации не может быть отказано:

а) когда заявление подано не соответствующим лицом;
б) по мотивам нецелесообразности;
в) даже если сведения в заявлении не соответствуют действительности;
г) если регистрирующий орган уже зарегистрировал другое средство массовой информации с тем же названием и формой распространения.

3. Засекречиванию подлежат сведения о:
а) состоянии демографии;
б) состоянии преступности;
в) фактах нарушения прав и свобод человека и гражданина;
г) силах и средствах гражданской обороны.

4. Проверить электронно-цифровую подпись под документом может:
а) только эксперт, преобразуя электронный образец документа и открытый ключ отправителя;
б) любое заинтересованное лицо, преобразуя электронный образец документа, открытый ключ отправителя и собственно значение электронно-цифровой подписи;
в) только эксперт с помощью преобразований электронного образца документа, открытого ключа отправителя и собственно значения электронно-цифровой подписи;
г) только отправитель электронного документа.

5. Режим документированной информации – это:
а) выделенная информация по определенной цели;
б) электронный документ с электронно-цифровой подписью;
в) выделенная информация в любой знаковой форме;
г) электронная информация, позволяющая ее идентифицировать.

6. Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется:
а) для доставки почтовых отправлений;
б) в целях профессиональной деятельности журналиста;
в) в целях профессиональной деятельности оператора;
г) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно.

7. Режим общественного достояния устанавливается для:
а) любой общедоступной информации;
б) сведений, которые являются уникальными, незаменимыми по своей природе;
в)любой общественной организации;
г)для государственных органов и муниципальных образований.

8. Учредителями средства массовой информации могут выступать:
а) граждане, достигшие 18 лет и лица без гражданства, постоянно проживающие на территории страны;
б) только юридические лица;
в) граждане, достигшие 16 лет и юридические лица;
г) граждане, достигшие 18 лет, объединения граждан, организаций, органы государственной власти.

9. Чтобы обеспечить доказательства при возникновении спора, редакция радио-, телепрограммы обязана сохранять в записи материалы собственных

передач, вышедших в эфир (не менее … со дня выхода в эфир) и фиксировать передачи, вышедшие в эфир в регистрационном журнале, который хранится не менее … с даты последней записи:

а) 1 месяца, 1 года;

б) 7 месяцев, полгода;

в) 1 года, 3 лет.

10. С точки зрения информационного права информация – это:

а) сведения о законодательстве, правовых явлениях, правоприменительной деятельности;

б) данные о развитии конкретной правовой науки и ее практическом применении;

в) сведения независимо от формы их представления;

г) форма выражения объективных знаний.

11. Не являются объектами информационного правоотношения:

а) неправовая информация;

б) обладатели информации;

в) информационные системы;

г) элементы информационной системы;

д) информационные продукты.

12. Общее управление информационной сферой не вправе осуществлять:

а) экспертные советы;

б) министерство информационных технологий;

в) федеральное агентство по науке и инновациям;

г) федеральные службы.

13.Открытость информации в архивных фондах обеспечивается:

а) различными режимами доступа к информации;

б) переходом информации из одной категории доступа в другую;

в) различными режимами доступа к информации и переходом информации из одной категории доступа в другую;

г) правовым статусом архивного фонда.

14. Под периодическим печатным изданием понимается альманах, бюллетень, имеющие:

а) постоянное название, текущий номер и выходящие в свет не реже одного раза в месяц;

б) постоянное название и выходящие в свет не реже одного раза в месяц;

в) постоянное название, текущий номер и выходящие в свет не реже одного раза в год;

г) постоянное название и текущий номер.

15. Признак, не относящийся к коммерческой тайне:

а) информация имеет действительную или потенциальную коммерческую ценность;

б) сведения, содержащие коммерческую тайну, устанавливаются учредительными документами;

в) отсутствует свободный доступ к информации;

г) обладатель информации принимает меры к охране ее конфиденциальности.

16. Основные объекты обеспечения информационной безопасности:

а) помещения, предназначенные для ведения закрытых переговоров;

б) информационные ресурсы, содержащие сведения, которые относятся к государственной тайне и конфиденциальной информации;
в) информационные продукты;
г) квалифицированные кадры в области информационных технологий.

17. Предмет информационного права на современном этапе развития законодательства – это:

а) информационные отношения, возникающие в процессе производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации;
б) совокупность результатов труда, воплощенных в информации, информационных ресурсов, информационных технологий, средств и технологий коммуникации информации по сетям связи;
в) продукты, производные от информации и деятельность, связанная с ними;
г) общественные отношения в информационной сфере.

18. К служебной тайне не относится:

а) профессиональная тайна;
б) тайна деятельности соответствующего органа;
в) вред, причиненный здоровью работника в связи с производственной травмой.

19. Вредоносные программы, выраженные в объективной форме и имеющие творческий характер, … охраноспособными:

а) являются;
б) не являются.

20. В правовой режим документированной информации входит:

а) государственная тайна;
б) тайна частной жизни;
в) банковская тайна;
г) электронная цифровая подпись;
д) персональные данные.

21. Исключите неправильный постулат:

а) информация не связана с определенным конкретным носителем;
б) информация не существует без материального носителя;
в) содержание информации меняется одновременно со сменой материального носителя.

22. Редакция обязана:

а) отвечать на письма граждан и пересылать письма тем органам, в чью компетенцию входит их рассмотрение;
б) соблюдать авторские права на результаты интеллектуальной деятельности;
в) в любом случае соблюдать в тайне источник информации с условием неразглашения его имени;
д) соблюдать в тайне источник информации с условием неразглашения его имени за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом;
е) распространить опровержение или предоставить гражданину право зачитать его самому, если затронуты честь, достоинство или деловая репутация гражданина.

23. К государственной тайне не относятся сведения, защищаемые государством …, распространение которых может нанести ущерб государству:

а) в экономической области;
б) в контрразведывательной деятельности;
в) в оперативно-разыскной деятельности;
г) о частной жизни политических деятелей.

24. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:

а) которые составляют финансово-экономическую информацию и позволяют избежать неоправданных расходов;
б) о безопасности пищевых продуктов;
в) о показателях производственного травматизма, профессиональной заболеваемости;
г) о системе оплаты и условиях труда.

25. Ответственность за создание вредоносной программы наступает в:

а) любом случае;
б) совокупности с ответственностью за ее использование;
в) случаях, установленных законодательством.

26. Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных:

а) осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник;
б) необходима в связи с осуществлением правосудия;
в) необходима в соответствии с оперативно-розыскной деятельностью;
г) необходима в связи с выездом за пределы страны.

27. Субъектами информационных отношений могут (может) быть:

а) муниципальные образования;
б) трудовой коллектив;
в) трансграничные информационно-телекоммуникационные сети.

28. Не является признаком информационного общества:

а) массовое подключение персональных компьютеров к трансграничным информационно-телекоммуникационным сетям;
б) мгновенная коммуникация членов общества друг с другом, вне зависимости от времени и от расстояния;
в) приоритетное развитие сельского хозяйства и промышленности на основе нанотехнологий;
г) общедоступность и постоянное обновление информационных данных.

29. Признак, не относящийся к охраноспособной информации – это:

а) охране подлежит только документированная информация;
б) доступ к охраноспособной информации ограничен только законом;
в) доступ к охраноспособной информации ограничен владельцем информационных ресурсов;
г) защита охраноспособной информации устанавливается ФЗ.

30. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:

а) о размере и составе имущества некоммерческих организаций;
б) об оплате труда работников некоммерческих организаций;

в) об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
г) об использовании новых технологий, позволяющих получить коммерческую выгоду.

31. Не являются принципами информационного права:

а) принцип оборотоспособности;
б) принцип распространяемости;
в) принцип свободы слова;
г) принцип равноправия языков;
д) принцип преимущества применения нанотехнологий в промышленности;
принцип имущественной ответственности.

32. Основное средство антивирусной защиты:

а) резервное копирование ценных данных;
б) регулярное сканирование жестких дисков;
в) подготовка квалифицированных кадров в сфере информационной безопасности.

33. Дети до 6 лет не вправе:

а) с согласия законных представителей пользоваться телефонными услугами;
б) с разрешения законных представителей выходить в Интернет;
в) с согласия законных представителей совершать сделки с компьютерной техникой.

34. Владелец информационных ресурсов не обязан:

а) бесплатно опубликовывать библиографическую информацию;
б) хранить производственные документы;
в) использовать информацию по своему усмотрению;
г) включать библиографическую информацию в международные автоматизированные банки данных.

35. Коммерческая тайна – это:

а) охраняемое законом право предприятия на ограниченный доступ к информации по производственным, технологическим, торговым, финансовым, другим хозяйственным операциям и документации по ним;
б) технические знания, опыт, секреты производства, необходимые для решения технической задачи.

36. Как показывает опыт работ зарубежных стран, наиболее уязвимым звеном в охране коммерческих секретов является:

а) незащищённость информационных систем;
б) персонал организации;
в) нерациональное отнесение сведений к коммерческой тайне предприятия.

37. Методы биометрической идентификации делятся на две большие группы:

а) статистические;
б) физиологические;
в) инерционные;
г) динамические.

38. Последовательное решение трех задач (проведение классификации объектов, определение форм и методов защиты и выбор способов контроля их эффективности) необходимо при разработке следующих мер:

а) защиты научно-технического потенциала;

б) защиты научно-технической собственности;
в) защиты активов, находящихся на балансе предприятия.

39. Все системы биометрической идентификации выполняют две основные функции:

а) регистрации;
б) идентификации;
в) архивирования;
г) систематизации.

40. **«Ламер» - это пользователь:**

а) необоснованно считающий себя специалистом;
б) начинающий пользователь;
в) опытный пользователь;
г) пользователь-специалист.

41. **Конфиденциальные сведения ранжируются по степени ограничения их распространения на:**

а) строго конфиденциальные сведения;
б) служебные сведения;
в) сведения общего пользования;
г) секретные сведения.

42.**Защищённые информационные системы основаны на:**

а) безотказности;
б) безопасности;
в) недоступности;
г) защищённости.

43.**Брандмауэр – это:**

а)совокупность аппаратных средств и программного обеспечения, связывающая две и большее количество сетей и являющаяся центральным пунктом управления безопасностью;

б) главный компьютер сети, выполняющий программное обеспечение, известное как сервер-посредник;

в) система, обеспечивающая регистрацию пользователей, формирование матрицы, доступа к вычислительным и информационным ресурсам сети.

44. **Одним из трёх наиболее популярных типов архитектуры брандмауэра является:**

а) односторонний главный брандмауэр;
б) двухсторонний главный брандмауэр;
в) трёхсторонний главный брандмауэр.

45. Режим документированной информации – это:

а) выделенная информация по определенной цели;
б) электронный документ с электронно-цифровой подписью;
в) выделенная информация в любой знаковой форме;
г) электронная информация, позволяющая ее идентифицировать.

46. Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется:

а) для доставки почтовых отправлений;
б) в целях профессиональной деятельности журналиста;

в) в целях профессиональной деятельности оператора;
г) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно.

47. Режим общественного достояния устанавливается для:

а) любой общедоступной информации;
б) сведений, которые являются уникальными, незаменимыми по своей природе;
в)любой общественной организации;
г)для государственных органов и муниципальных образований.

48. Учредителями средства массовой информации могут выступать:

а) граждане, достигшие 18 лет и лица без гражданства, постоянно проживающие на территории страны;
б) только юридические лица;
в) граждане, достигшие 16 лет и юридические лица;
г) граждане, достигшие 18 лет, объединения граждан, организаций, органы государственной власти.

49. Чтобы обеспечить доказательства при возникновении спора, редакция радио-, телепрограммы обязана сохранять в записи материалы собственных передач, вышедших в эфир (не менее … со дня выхода в эфир) и фиксировать передачи, вышедшие в эфир в регистрационном журнале, который хранится не менее … с даты последней записи:

а) 1 месяца, 1 года;
б) 7 месяцев, полгода;
в) 1 года, 3 лет.

50. С точки зрения информационного права информация – это:

а) сведения о законодательстве, правовых явлениях, правоприменительной деятельности;
б) данные о развитии конкретной правовой науки и ее практическом применении;
в) сведения независимо от формы их представления;
г) форма выражения объективных знаний.

51. Режим защиты информации не устанавливается в отношении сведений, относящихся к:

а) государственной тайне;
б) деятельности государственных деятелей;
в) конфиденциальной информации;
г) персональным данным.

52. В регистрации средства массовой информации не может быть отказано:

а) когда заявление подано не соответствующим лицом;
б) по мотивам нецелесообразности;
в) даже если сведения в заявлении не соответствуют действительности;
г) если регистрирующий орган уже зарегистрировал другое средство массовой информации с тем же названием и формой распространения.

53. Засекречиванию подлежат сведения о:

а) состоянии демографии;
б) состоянии преступности;
в) фактах нарушения прав и свобод человека и гражданина;
г) силах и средствах гражданской обороны.

54. Проверить электронно-цифровую подпись под документом может:
а) только эксперт, преобразуя электронный образец документа и открытый ключ отправителя;
б) любое заинтересованное лицо, преобразуя электронный образец документа, открытый ключ отправителя и собственно значение электронно-цифровой подписи;
в) только эксперт с помощью преобразований электронного образца документа, открытого ключа отправителя и собственно значения электронно-цифровой подписи;
г) только отправитель электронного документа.
55. Режим документированной информации – это:
а) выделенная информация по определенной цели;
б) электронный документ с электронно-цифровой подписью;
в) выделенная информация в любой знаковой форме;
г) электронная информация, позволяющая ее идентифицировать.
56. Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется:
а) для доставки почтовых отправлений;
б) в целях профессиональной деятельности журналиста;
в) в целях профессиональной деятельности оператора;
г) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно.
57. Режим общественного достояния устанавливается для:
а) любой общедоступной информации;
б) сведений, которые являются уникальными, незаменимыми по своей природе;
в)любой общественной организации;
г)для государственных органов и муниципальных образований.
58. Учредителями средства массовой информации могут выступать:
а) граждане, достигшие 18 лет и лица без гражданства, постоянно проживающие на территории страны;
б) только юридические лица;
в) граждане, достигшие 16 лет и юридические лица;
г) граждане, достигшие 18 лет, объединения граждан, организаций, органы государственной власти.
59. Чтобы обеспечить доказательства при возникновении спора, редакция радио-, телепрограммы обязана сохранять в записи материалы собственных передач, вышедших в эфир (не менее … со дня выхода в эфир) и фиксировать передачи, вышедшие в эфир в регистрационном журнале, который хранится не менее … с даты последней записи:
а) 1 месяца, 1 года;
б) 7 месяцев, полгода;
в) 1 года, 3 лет.
60. С точки зрения информационного права информация – это:
а) сведения о законодательстве, правовых явлениях, правоприменительной деятельности;
б) данные о развитии конкретной правовой науки и ее практическом применении;

в) сведения независимо от формы их представления;
г) форма выражения объективных знаний.

61. Не являются объектами информационного правоотношения:

а) неправовая информация;
б) обладатели информации;
в) информационные системы;
г) элементы информационной системы;
д) информационные продукты;
е) недокументированная информация.

62. Общее управление информационной сферой не вправе осуществлять:

а) экспертные советы;
б) министерство информационных технологий;
в) федеральное агентство по науке и инновациям;
г) федеральные службы.

63.Открытость информации в архивных фондах обеспечивается:

а) различными режимами доступа к информации;
б) переходом информации из одной категории доступа в другую;
в) различными режимами доступа к информации и переходом информации из одной категории доступа в другую;
г) правовым статусом архивного фонда.

64. Под периодическим печатным изданием понимается альманах, бюллетень, имеющие:

а) постоянное название, текущий номер и выходящие в свет не реже одного раза в месяц;
б) постоянное название и выходящие в свет не реже одного раза в месяц;
в) постоянное название, текущий номер и выходящие в свет не реже одного раза в год;
г) постоянное название и текущий номер.

65. Признак, не относящийся к коммерческой тайне:

а) информация имеет действительную или потенциальную коммерческую ценность;
б) сведения, содержащие коммерческую тайну, устанавливаются учредительными документами;
в) отсутствует свободный доступ к информации;
г) обладатель информации принимает меры к охране ее конфиденциальности.

66. Основные объекты обеспечения информационной безопасности:

а) помещения, предназначенные для ведения закрытых переговоров;
б) информационные ресурсы, содержащие сведения, которые относятся к государственной тайне и конфиденциальной информации;
в) информационные продукты;
г) квалифицированные кадры в области информационных технологий.

67. Предмет информационного права на современном этапе развития законодательства – это:

а) информационные отношения, возникающие в процессе производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации;

б) совокупность результатов труда, воплощенных в информации, информационных ресурсов, информационных технологий, средств и технологий коммуникации информации по сетям связи;
в) продукты, производные от информации и деятельность, связанная с ними
г) общественные отношения в информационной сфере.

68. К служебной тайне не относится:
а) профессиональная тайна;
б) тайна деятельности соответствующего органа;
в) вред, причиненный здоровью работника в связи с производственной травмой.

69. Вредоносные программы, выраженные в объективной форме и имеющие творческий характер, … охраноспособными:
а) являются;
б) не являются.

70. В правовой режим документированной информации входит:
а) государственная тайна;
б) тайна частной жизни;
в) банковская тайна;
г) электронная цифровая подпись;
д) персональные данные.

71. Исключите неправильный постулат:
а) информация не связана с определенным конкретным носителем;
б) информация не существует без материального носителя;
в) содержание информации меняется одновременно со сменой материального носителя.

72. Редакция обязана:
а) отвечать на письма граждан и пересылать письма тем органам, в чью компетенцию входит их рассмотрение;
б) соблюдать авторские права на результаты интеллектуальной деятельности;
в) в любом случае соблюдать в тайне источник информации с условием неразглашения его имени;
д) соблюдать в тайне источник информации с условием неразглашения его имени за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом;
е) распространить опровержение или предоставить гражданину право зачитать его самому, если затронуты честь, достоинство или деловая репутация гражданина.

73. К государственной тайне не относятся сведения, защищаемые государством …, распространение которых может нанести ущерб государству:
а) в экономической области;
б) в контрразведывательной деятельности;
в) в оперативно-разыскной деятельности;
г) о частной жизни политических деятелей.

74. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:
а) которые составляют финансово-экономическую информацию и позволяют избежать неоправданных расходов;
б) о безопасности пищевых продуктов;

в) о показателях производственного травматизма, профессиональной заболеваемости;
г) о системе оплаты и условиях труда.

75. Ответственность за создание вредоносной программы наступает в:

а) любом случае;
б) совокупности с ответственностью за ее использование;
в) случаях, установленных законодательством.

76. Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных:

а) осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник;
б) необходима в связи с осуществлением правосудия;
в) необходима в соответствии с оперативно-розыскной деятельностью;
г) необходима в связи с выездом за пределы страны.

77. Субъектами информационных отношений могут (может) быть:

а) муниципальные образования;
б) трудовой коллектив;
в) трансграничные информационно-телекоммуникационные сети.

78. Не является признаком информационного общества:

а) массовое подключение персональных компьютеров к трансграничным информационно-телекоммуникационным сетям;
б) мгновенная коммуникация членов общества друг с другом, вне зависимости от времени и от расстояния;
в) приоритетное развитие сельского хозяйства и промышленности на основе нанотехнологий;
г) общедоступность и постоянное обновление информационных данных.

79. Признак, не относящийся к охраноспособной информации – это:

а) охране подлежит только документированная информация;
б) доступ к охраноспособной информации ограничен только законом;
в) доступ к охраноспособной информации ограничен владельцем информационных ресурсов;
г) защита охраноспособной информации устанавливается ФЗ.

80. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:

а) о размере и составе имущества некоммерческих организаций;
б) об оплате труда работников некоммерческих организаций;
в) об использовании безвозмездного труда граждан в деятельности некоммерческой организации;
г) об использовании новых технологий, позволяющих получить коммерческую выгоду.

81. Не являются принципами информационного права:

а) принцип оборотоспособности;
б) принцип распространяемости;
в) принцип свободы слова;
г) принцип равноправия языков.

82. Основное средство антивирусной защиты:
а) **резервное копирование ценных данных;**
б) регулярное сканирование жестких дисков;
в) подготовка квалифицированных кадров в сфере информационной безопасности.
83. Дети до 6 лет не вправе:
а) с согласия законных представителей пользоваться телефонными услугами;
б) с разрешения законных представителей выходить в Интернет;
в) с согласия законных представителей совершать сделки с компьютерной техникой.
84. Владелец информационных ресурсов не обязан:
а) бесплатно опубликовывать библиографическую информацию;
б) хранить производственные документы;
в) использовать информацию по своему усмотрению;
г) включать библиографическую информацию в международные автоматизированные банки данных.
85. Коммерческая тайна – это:
а) охраняемое законом право предприятия на ограниченный доступ к информации по производственным, технологическим, торговым, финансовым, другим хозяйственным операциям и документации по ним;
б) технические знания, опыт, секреты производства, необходимые для решения технической задачи.
86. Как показывает опыт работ зарубежных стран, наиболее уязвимым звеном в охране коммерческих секретов является:
а) незащищённость информационных систем;
б) персонал организации;
в) нерациональное отнесение сведений к коммерческой тайне предприятия.
87. Методы биометрической идентификации делятся на две большие группы:
а) статистические;
б) физиологические;
в) инерционные;
г) динамические.
88. Последовательное решение трех задач (проведение классификации объектов, определение форм и методов защиты и выбор способов контроля их эффективности) необходимо при разработке следующих мер:
а) защиты научно-технического потенциала;
б) защиты научно-технической собственности;
в) защиты активов, находящихся на балансе предприятия.
89. Все системы биометрической идентификации выполняют две основные функции:
а) регистрации;
б) идентификации;
в) архивирования;
г) систематизации.
90. **«Ламер» - это пользователь:**
а) необоснованно считающий себя специалистом;
б) начинающий пользователь;

в) опытный пользователь;
г) пользователь-специалист.
91.**Конфиденциальные сведения ранжируются по степени ограничения их распространения на:**
а) строго конфиденциальные сведения;
б) служебные сведения;
в) сведения общего пользования;
г) секретные сведения.
92.**Защищённые информационные системы основаны на:**
а) безотказности;
б) безопасности;
в) недоступности;
г) защищённости.
93. Брандмауэр – это:
а) совокупность аппаратных средств и программного обеспечения, связывающая две и большее количество сетей и являющаяся центральным пунктом управления безопасностью;
б) главный компьютер сети, выполняющий программное обеспечение, известное как сервер-посредник;
в) система, обеспечивающая регистрацию пользователей, формирование матрицы, доступа к вычислительным и информационным ресурсам сети.
94. Одним из трёх наиболее популярных типов архитектуры брандмауэра является:
односторонний главный брандмауэр;
двухсторонний главный брандмауэр;
трёхсторонний главный брандмауэр.
95. Режим документированной информации – это:
а) выделенная информация по определенной цели;
б) электронный документ с электронно-цифровой подписью;
в) выделенная информация в любой знаковой форме;
г) электронная информация, позволяющая ее идентифицировать.
96. Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется:
а) для доставки почтовых отправлений;
б) в целях профессиональной деятельности журналиста;
в) в целях профессиональной деятельности оператора;
г) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно
97. Режим общественного достояния устанавливается для:
а) любой общедоступной информации;
б) сведений, которые являются уникальными, незаменимыми по своей природе;
в) любой общественной организации;
г) для государственных органов и муниципальных образований.
98. Учредителями средства массовой информации могут выступать:
а) граждане, достигшие 18 лет и лица без гражданства, постоянно проживающие на территории страны;

б) только юридические лица;
в) граждане, достигшие 16 лет и юридические лица;
г) граждане, достигшие 18 лет, объединения граждан, организаций, органы государственной власти.

99. Чтобы обеспечить доказательства при возникновении спора, редакция радио-, телепрограммы обязана сохранять в записи материалы собственных передач, вышедших в эфир (не менее … со дня выхода в эфир) и фиксировать передачи, вышедшие в эфир в регистрационном журнале, который хранится не менее … с даты последней записи:

а) 1 месяца, 1 года;
б) 7 месяцев, полгода;
в) 1 года, 3 лет.

100. С точки зрения информационного права информация – это:

а) сведения о законодательстве, правовых явлениях, правоприменительной деятельности;
б) данные о развитии конкретной правовой науки и ее практическом применении;
в) сведения независимо от формы их представления;
г) форма выражения объективных знаний.

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры, на котором были рассмотрены и одобрены изменения и дополнения.	Подпись (с расшифровкой) заведующего кафедрой