Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Факультет искусственного интеллекта

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(направленность (профиль) ОП ВО)

Москва, 2025

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

1. Виды контроля по периодам обучения

2.1 Материалы для проведения текущего контроля.

2.1.1. Форма текущего контроля – письменный экспресс-опрос на семинаре с выставлением оценок в балльной системе

2.1.2. Перечень вопросов (заданий).

Задание № 1. Назначение и структура правового обеспечения информационной безопасности.

Вопрос № 1. Угрозы информационной безопасности и условия правового обеспечения их нейтрализации.

Вопрос № 2. Объекты и методы обеспечения информационной безопасности.

Вопрос № 3. Социальные нормы в обеспечении информационной безопасности: моральные, правовые, политические, эстетические, корпоративные. Технико-правовые нормы и роль технического регулирования в обеспечении информационной безопасности.

Вопросы для самоконтроля:

1. Информационная безопасность как предмет реализации мер правового и организационного обеспечения.

2. Содержание мер организационного и правового обеспечения информационной безопасности.

3 Система правовых норм в сфере обеспечения информационной безопасности.

Проблемные вопросы:

1. Понятие об информационном объекте и его элементах.

2. Концептуальные основы формирования системы обеспечения информационной безопасности.

3. Роль либертарного права в регулировании отношений в информационной сфере.

Задание № 2. Правовое регулирование отношений в интересах обеспечения информационной безопасности.

Вопрос № 1. Основы правового обеспечения информационной безопасности. Отрасли права, обеспечивающие законность в интересах информационной безопасности. Структура и направленность правовых мер обеспечения информационной безопасности.

Вопрос № 2. Информационная сфера как сфера обращения информации и правового регулирования. Субъекты и объекты информационного права. Система и нормы информационного права. Правонарушения в информационной сфере.

Вопрос № 3. Международно-правовые акты и международные стандарты в области информационной безопасности. Окинавская хартия глобального информационного общества. Соглашение участников СНГ по информационной безопасности. Международные стандарты по информационной безопасности.

Вопрос № 4. Информационное законодательство как основной источник информационного права. Федеральные законы, Указы Президента РФ и Постановления Правительства о защите интеллектуальной собственности, о государственной тайне, о коммерческой тайне, о персональных данных. Информационно-правовые нормы конституционного, административного, гражданского, трудового и уголовного законодательства в сфере информационной безопасности.

Вопрос № 5. Особенности ведомственного и корпоративного нормативного регулирования обеспечения информационной безопасности. Действующие нормативные правовые акты в системе обеспечения информационной безопасности и защиты информации. Формирование корпоративных требований и спецификаций информационной безопасности.

Вопросы для самоконтроля:

1. Теории и источники права.
2. Правовая система и система права.
3. Структура правовой нормы.
4. Правовая классификация информационных ресурсов, продуктов и услуг.
5. Понятие и назначение информационного права.
6. Информационные отношения.
7. Методы правового регулирования и принципы информационного права.
8. Установления основных информационных правовых норм в Конституции Российской Федерации.
9. Акты отрасли информационного законодательства Российской Федерации.
10. Отрасли российского законодательства, акты которых включают отдельные информационно-правовые нормы.
11. Сущность ведомственного правового акта и его государственная регистрация.
12. Сущность, роль и место политик безопасности в деятельности предприятия.
13. Структура корпоративной политики информационной безопасности.

Проблемные вопросы:

1. Право и его роль в регулировании комплекса отношений в информационной сфере, объекты и субъекты правоотношений.
2. Юридические особенности и свойства информации.
3. Проблемы принятия международных конвенций по информационной безопасности.
4. Исходные данные для формирования политики информационной безопасности предприятия.

Задание № 3. Правовые основы защиты государственной, коммерческой, служебной, профессиональной тайны и персональных данных.

Вопрос № 1. Защита тайны в системе защиты информации. Правовые основы защиты государственной тайны. Закон РФ «О государственной тайне» и действующие нормативные правовые акты, нормативно-методические и методические документы в системе защиты государственной тайны.

Вопрос № 2. Правовой институт отнесения сведений к государственной тайне. Перечень сведений, составляющих государственную тайну. Права обладателя информации, составляющей коммерческую тайну.

Вопрос № 3. Степени и грифы секретности. Засекречивание и рассекречивание. Допуск к государственной тайне и к конфиденциальной информации.

Вопрос № 4. Действующие нормативные правовые акты о лицензировании. Цели, задачи лицензирования отдельных видов деятельности. Лицензионные требования, предъявляемые к соискателю лицензии и лицензиату по технической защите конфиденциальной информации

Вопрос № 5. Действующие нормативные правовые акты о сертификации деятельности, связанной с государственной тайной и защитой информации. Место и роль сертификации в техническом регулировании. Содержание сертификации средств защиты информации по требованиям безопасности информации.

Вопрос № 6. Система правовой ответственности за утечку информации и утрату носителей информации. Виды и условия применения правовых норм гражданско-правовой, административной и дисциплинарной ответственности за разглашение защищаемой информации и невыполнение правил ее защиты. Уголовно-правовая и криминалистическая характеристика компьютерных преступлений. Уголовная ответственность за компьютерные преступления.

Вопросы для самоконтроля:

1. Принципы защиты государственной тайны.
2. Перечни сведений, отнесенных к государственной тайне.
3. Перечень сведений, составляющих коммерческую тайну.

4. Сведения, которые не могут составлять государственную и коммерческую тайну.

5. Основания и порядок доступа к конфиденциальной информации.

6. Основные принципы и полномочия осуществления лицензирования.

7. Перечень видов деятельности, на которые требуются лицензии в интересах защиты государственной тайны.

8. Обязательная сертификация и ее организация.

9. Аккредитация органов по сертификации и испытательных лабораторий (центров).

10. Понятие и классификация компьютерных преступлений.

Проблемные вопросы:

1. Отнесение сведений к коммерческой, служебной и профессиональной тайнам.

2. Критерии определения лицензируемых видов деятельности.

3. Уточнение перечня средств защиты информации, подлежащих сертификации.

4. Расследование компьютерных преступлений.

Задание № 4. Правовые аспекты защиты прав обладателей информации.

Вопрос № 1. Право владения, право пользования и право распоряжения информацией. Система защиты прав обладателя собственности на информацию.

Вопрос № 2. Понятие интеллектуальной собственности и ее виды. Интеллектуальный продукт. Государственная регистрация интеллектуальной собственности. Содержание гражданско-правовых норм в области защиты интеллектуальной собственности. Ответственность юридических лиц и индивидуальных предпринимателей за нарушения исключительных прав.

Вопрос № 3. Действие исключительного авторского права на произведения науки, литературы и искусства на территории Российской Федерации. Автор и соавтор произведения. Свободное воспроизведение программ для ЭВМ и баз данных. Декомпилирование программ для ЭВМ. Программы для ЭВМ и базы данных, созданные по заказу и при выполнении работ по договору. Информация об авторском праве. Обеспечение иска по делам о нарушении авторских прав.

Вопрос № 4. Понятие и срок исполнения договора авторского заказа. Лицензионный договор о предоставлении права использования произведения. Особые условия издательского лицензионного договора. Ответственность по договорам, заключаемым автором.

Вопрос № 5. Распоряжение исключительным правом на изобретение, полезную модель или промышленный образец, созданных в связи с выполнением служебного задания и при выполнении работ по договору. Получение патента, прекращение и восстановление его действия. Защита прав авторов и патентообладателей.

Вопрос № 6. Особенности правовой охраны коллективного знака. Прекращение исключительного права на товарный знак.

Вопросы для самоконтроля:

1. Права и обязанности обладателя информации.

2. Способы защиты интеллектуальных прав.

3. Защита личных неимущественных прав и исключительных прав.

4. Объекты авторских прав.

5. Программы для ЭВМ как объект авторских прав.

6. Договор об отчуждении исключительного права на произведение.

7. Особенности правовой охраны общеизвестного товарного знака.

Проблемные вопросы:

1. Судебная защита и самозащита прав обладателя собственности на информацию.

2. Реализация интеллектуальных прав.

3. Применение технических средств защиты авторских прав.

4. Защита права на товарный знак.

Задание №5. Содержание организационного обеспечения информационной безопасности.

Вопрос № 1. Условия и факторы, оказывающие влияние на организационную структуру системы обеспечения информационной безопасности. Требования международных стандартов по вопросам организации обеспечения информационной безопасности. Политики безопасности. Роли высших корпоративных органов управления, менеджеров, службы информационной безопасности, сотрудников, внешних контролирующих органов в системе обеспечения информационной безопасности.

Вопрос № 2. Место структурного подразделения защиты государственной тайны в системе защиты государственной тайны предприятия. Задачи и методы работы подразделений защиты государственной тайны.

Вопрос № 3. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Проверочные мероприятия, обучение работе с конфиденциальной информацией и оформление допуска к ней при приеме на работу. Правовое регулирование взаимоотношений администрации и персонала при инцидентах нарушения информационной безопасности.

Вопросы для самоконтроля:

1. Принципы организационного обеспечения информационной безопасности.
2. Силы и средства обеспечения информационной безопасности.
3. Правовые основы деятельности подразделений защиты информации на предприятии.
4. Мониторинг осведомленности персонала о тайнах работодателя.
5. Обязанности администрации по созданию надлежащих условий персоналу для работы с конфиденциальной информацией.
6. Обязанности администрации по сохранности персональных данных сотрудников.
7. Добровольное обязательство сотрудника по неразглашению тайны.
8. Права и обязанности персонала при работе в области защиты информации.

Проблемные вопросы:

1. Роль и возможности акционеров по формированию требований к информационной безопасности корпорации и контролю эффективности их выполнения.
2. Порядок проведения дознания по инцидентам нарушения информационной безопасности.
3. Порядок возмещения ущерба от нарушения информационной безопасности.

Задание № 6. Организация внутриобъектового, пропускного режима и охраны предприятия.

Вопрос № 1. Понятие и принципы организации внутриобъектового режима. Функциональные зоны: методика разграничения и методы обособления. Контрольно-пропускной пункт: оборудование и организация дежурства. Бюро пропусков и виды пропуска.

Вопрос № 2. Организационные меры по предотвращению проникновения посторонних лиц на предприятие. Защита жизни и здоровья персонала.

Вопрос № 3. Противопожарная охрана. Организация эвакуации персонала и конфиденциальных документов в чрезвычайных ситуациях. Охрана конфиденциальных документов и имущества при транспортировке.

Вопрос № 4. Требования к помещению для проведения совещаний и заседаний по конфиденциальным вопросам. Мероприятия по исключению утечки информации по техническим каналам, через виброакустические проводники и посредством видеонаблюдения.

Вопросы для самоконтроля:

1. Понятие и принципы организации пропускного режима.
2. Средства охраны.
3. Мероприятия по исключению закладок разведывательных электронных устройств.
4. Мероприятия по обнаружению включенных электронных приборов у участников совещания.

Проблемные вопросы:

1. Охрана территории предприятия и функциональных зон от проникновения нарушителей.

2. Обеспечение порядка в местах массовых мероприятий.

3. Профилактическая работа с участниками совещаний и заседаний по конфиденциальным вопросам.

Задание № 7. Обеспечение информационной безопасности при работе со СМИ и в рекламной деятельности.

Вопрос № 1. Роль органов управления, пресс-службы и службы защиты информации в недопущении утечки конфиденциальной информации через СМИ.

Вопрос № 2. Роль органов управления, рекламной службы и службы защиты информации в недопущении утечки конфиденциальной информации в рекламной деятельности.

Вопросы для самоконтроля:

1. Условия, способствующие нежелательной публикации в СМИ конфиденциальной информации.

2. Условия, способствующие утечке конфиденциальной информации в рекламной деятельности.

Проблемные вопросы:

1. Информационная безопасность персонала при работе со СМИ.

2. Противодействие манипуляции в ходе восприятия потребительской рекламы и при заключении деловых соглашений.

Задание № 8. Организация аналитической работы по предупреждению утечки конфиденциальной информации.

Вопрос № 1. Методы сбора информации об уязвимостях системы защиты информации и об устремлениях нарушителей.

Вопрос № 2. Оценка рисков информационной безопасности.

Вопросы для самоконтроля:

1. Источники информации об уровне информационной безопасности.

2. Методы систематизации информации.

Проблемные вопросы:

1. Оценка достоверности сведений.

2. Аналитическое выявление угроз информационной безопасности.

Вариант теста по оценке знаний:

1. Согласно Конституции Российской Федерации право на информацию составляют следующие правомочия:

а) право искать и получать информацию;

б) право производить и распространять информацию, информационные ресурсы и информационные системы;

в) право искать, получать, передавать, производить и распространять информацию.

2. Предмет правового обеспечения информационной безопасности составляют:

а) общественные отношения, связанные с защитой информации, при использовании информационных ресурсов и информационных систем;

б) общественные отношения в области сертификации видов защиты информации;

в) общественные отношения в области обеспечения государственной тайны.

3. В законодательстве Российской Федерации информация определяется как:

а) мера неоднородности распределения материи и энергии в пространстве и во времени;

б) обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему;

в) сведения (сообщения, данные) независимо от формы их представления.

4. Систему правового обеспечения информационной безопасности составляют:

а) Конституция Российской Федерации, федеральные конституционные и федеральные законы, указы Президента Российской Федерации, постановления Правительства Российской Федерации, ведомственные правовые акты;

б) Конституция Российской Федерации, федеральные конституционные и федеральные законы, указы Президента Российской Федерации, постановления Правительства Российской Федерации, нормативные правовые акты, принимаемые органами государственной власти субъектов Российской Федерации, ведомственные правовые акты;

в) Конституция Российской Федерации, федеральные конституционные и федеральные законы, указы Президента Российской Федерации, постановления Правительства Российской Федерации

5. Согласно Конституции Российской Федерации в ведении Российской Федерации находятся:

а) государственные информационные ресурсы;

б) федеральные информация и связь;

в) государственные информационные системы.

6. Конституцией Российской Федерации закреплено право граждан на достоверную информацию:

а) о состоянии здоровья высших должностных лиц Российской Федерации;

б) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

в) о состоянии окружающей природной среды;

7. Согласно Конституции Российской Федерации неопубликованные законы:

а) не применяются;

б) применяются в части, не противоречащей опубликованным;

в) применяются наравне с опубликованными.

8. Согласно Конституции Российской Федерации официальному опубликованию подлежат:

а) законы и иные нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина;

б) экземпляры различных видов документов, изготовленных по заказу организаций и отдельных лиц, которые подлежат безвозмездной передаче их производителями в соответствующие организации в порядке и количестве, установленных федеральным законом;

в) предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

9. Окинавская хартия глобального информационного общества была подписана:

а) Б.Н. Ельциным

б) В.В. Путиным

в) Д.А. Медведевым

10. Обязательным условием включения информации в информационные ресурсы является:

а) открытость информации;

б) документирование информации;

в) экспертная оценка информации.

11. В соответствии со сферами ведения к государственным информационным системам относятся:

а) информационные системы органов государственной власти, юридических и физических лиц;

б) федеральные информационные системы, информационные системы, находящиеся в совместном ведении Российской Федерации и субъектов Российской Федерации и информационные системы субъектов Российской Федерации;

в) федеральные информационные системы, информационные системы субъектов Российской Федерации и муниципальные информационные системы.

12. В зависимости от порядка документирования информации, категории информации по уровню доступа к ней и правил защиты информации информационные ресурсы различаются по:

а) правовому режиму;

б) правовому статусу;

в) правовому принципу.

13. Государственные информационные ресурсы (за исключением информации с ограниченным доступом) являются:

а) открытыми и общедоступными;

б) служебной информацией;

в) массовой информацией.

14. Не может быть ограничен доступ к:

а) информации о состоянии окружающей среды;

б) о частной жизни человека и гражданина;

в) информации, полученной гражданами при исполнении своих профессиональных обязанностей.

15. Персональные данные (информация о гражданах) определены в законодательстве Российской Федерации как:

а) фамилия, имя, отчество, дата рождения, место жительства;

б) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование,

профессия, доходы, другая информация;

в) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

16. Согласно законодательству Российской Федерации к государственной тайне относятся:

а) защищаемые государством сведения, распространение которых может нанести ущерб безопасности Российской Федерации;

б) защищаемые государством информационные ресурсы, доступ к которым которых может нанести ущерб безопасности Российской Федерации;

в) защищаемые государством информационные системы, доступ к которым может нанести ущерб безопасности Российской Федерации.

17. Перечень сведений, составляющих государственную тайну, определяется:

а) федеральным законом;

б) постановлением Правительства Российской Федерации;

в) международным договором

18. К информации с ограниченным доступом запрещено относить:

а) документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

б) сведения о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

в) научно-техническую, технологическую, производственную, финансово-экономическую или иную информацию, которая имеет действительную или потенциальную коммерческую ценность.

19. В качестве самостоятельного вида объектов гражданских прав в Гражданском кодексе Российской Федерации выделены:

а) информация;

б) информационные ресурсы;

в) информационные системы.

20. Гражданским кодексом Российской Федерации регулируются правоотношения, связанные:

а) с государственной тайной;

б) со служебной и коммерческой тайной;

в) с персональными данными.

21. Коммерческую тайну составляют:

а) произведение искусства, перенесенное на предметы практического пользования, включая произведение художественного промысла или произведение, изготовляемое промышленным способом;

б) научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны;

в) зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними.

22. Преступлением, согласно уголовному законодательству Российской Федерации, считается:

а) нарушение порядка сбора и обработки персональных данных;

б) нарушение неприкосновенности частной жизни;

в) нарушение порядка работы с конфиденциальной информацией

23. В соответствии с законодательством Российской Федерации информационной системой является:

а) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

б) программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; другая эксплуатационная и сопроводительная документация);

в) организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

24. В целях информирования граждан и организаций в Российской Федерации осуществляется государственный учет:

а) информационных ресурсов;

б) информационных систем;

в) баз данных и банков данных.

25. В соответствии с законодательством Российской Федерации электронным документом является:

а) документ, в котором информация представлена в электронно-цифровой форме;

б) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;

в) объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

26. Согласно законодательству, как реквизит электронного документа электронная цифровая подпись призвана обеспечить:

а) защиту электронного документа от подделки и идентификацию владельца сертификата ключа подписи;

б) признание электронного документа доказательством в суде;

в) признание нотариальной письменной формы сделки.

27. В соответствии с законодательством Российской Федерации защите подлежит информация:

а) отнесенная к государственной тайне;

б) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу;

в) предназначенная для неограниченного круга лиц.

28. Под информационной безопасностью в законодательстве Российской Федерации понимается:

а) состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства;

б) состояние защищенности информации от несанкционированного доступа к данной информации, а также от нарушения функционирования программно-технических средств сбора, обработки, накопления, хранения, поиска и передачи информации или от вывода указанных средств из строя, обеспеченное совокупностью мер и средств защиты информации;

в) сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством.

29. Под угрозой безопасности в соответствии с законодательством понимается:

а) мера опасности, включающая вероятность возникновения чрезвычайной ситуации и ущерб, полученный в результате ее реализации;

б) совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства;

в) применение вооруженной силы иностранным государством (группой государств) против суверенитета, политической независимости и территориальной целостности Российской Федерации.

30. Официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации изложены в

а) Стратегии национальной безопасности Российской Федерации;

б) Доктрине информационной безопасности Российской Федерации;

в) Концепции развития документальной электросвязи.

31. К универсальным услугам связи относятся:

а) услуги по передаче данных и предоставлению доступа к сети «Интернет» с использованием пунктов коллективного доступа;

б) передача и получение информационных продуктов, а также оказание информационных услуг через Государственную границу Российской Федерации;

в) услуги по выдаче участникам информационных систем сертификатов ключей подписей, зарегистрированных удостоверяющим центром, одновременно с информацией об их действии в форме электронных документов.

32. Обладатель документированной информации обязан предоставлять бесплатно:

а) информацию о деятельности государственных органах и органах местного самоуправления, размещенную ими в информационно-телекоммуникационных сетях;

б) доступ к открытым информационным ресурсам;

в) доступ ко всей имеющейся у него информации.

33. Информационная система общего пользования это:

а) совокупность периодических аудио-, аудиовизуальных сообщений и материалов (передач), имеющая постоянное название и выходящая в свет (в эфир) не реже одного раза в год;

б) сеть связи, предназначенная для возмездного оказания услуг электросвязи любому пользователю услугами связи на территории Российской Федерации;

в) информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

34. Общедоступная библиотека предоставляет возможность пользования ее фондом и услугами:

а) юридическим лицам независимо от их организационно-правовых форм и форм собственности и гражданам без ограничений по уровню образования, специальности, отношению к религии;

б) гражданам независимо от пола, расы, национальности, языка, происхождения, имущественного и должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также других обстоятельств;

в) юридическим лицам независимо от организационно-правовой формы.

35. К объектам охраны авторских прав относятся:

а) информационная система;

б) программа для ЭВМ;

в) информационные технологии.

36. Официальным источником опубликования федеральных законов, актов Президента Российской Федерации и актов Правительства Российской Федерации является:

а) газета «Новая газета»;

б) средство массовой информации, продукция которого предназначена для распространения преимущественно: на всей территории Российской Федерации, за ее пределами, на территориях нескольких субъектов Российской Федерации;

в) «Российская газета» и «Собрание законодательства Российской Федерации».

37. Преступлениям в сфере компьютерной информации в Уголовном кодексе Российской Федерации посвящена:

а) 28 глава;

б) 146 статья;

в) 27 глава.

38. В качестве санкции (наказания) Кодекс об административных правонарушениях РФ использует:

а) лишение свободы;

б) штраф;

в) конфискацию имущества.

39. Увольнение с работы происходит в соответствии с нормами:

а) Гражданского кодекса РФ;

б) Кодекса об административных правонарушениях;

в) Трудового кодекса РФ.

40. Кто проводит экспертизу компьютерных преступлений во время судебного процесса:

а) прокуратура;

б) милиция;

в) судебно-экспертное учреждение.

Правильные ответы на вопросы теста.

№ вопроса	Правильный вариант ответа	№ вопроса	Правильный вариант ответа	№ вопроса	Правильный вариант ответа	№ вопроса	Правильный вариант ответа	№ вопроса	Правильный вариант ответа
1.	В	9.	Б	17.	А	25.	А	33.	В
2.	А	10.	Б	18.	А	26.	А	34.	Б
3.	В	11.	Б	19.	А	27.	Б	35.	Б
4.	Б	12.	А	20.	Б	28.	А	36.	В
5.	Б	13.	А	21.	Б	29.	Б	37.	А
6.	В	14.	А	22.	Б	30.	Б	38.	Б
7.	А	15.	Б	23.	А	31.	А	39.	В
8.	А	16.	А	24.	В	32.	Б	40.	В

2.2 Материалы для проведения промежуточной аттестации:

Четвертый семестр.

Вид промежуточной аттестации – дифференцированный зачет.

Форма проведения – устный опрос.

Перечень тем, вопросов, практических заданий, выносимых на промежуточную аттестацию:

1. Сущность, содержание понятий «опасность» и «безопасность», факторы, оказывающие влияние на информационную безопасность.
2. Топология информационного объекта и содержание ее элементов социотехнического информационного объекта.
3. Представить в виде схемы и прокомментировать методический аппарат формирования системы обеспечения информационной безопасности.
4. Методы обеспечения информационной безопасности Российской Федерации.
5. Цели и задачи обеспечения информационной безопасности предприятия.
6. Содержание организационных основ обеспечения информационной безопасности предприятия.
7. Силы, обеспечивающие информационную безопасность предприятия, роль и задачи службы обеспечения информационной безопасности.
9. Средства обеспечения информационной безопасности предприятия.
10. Технологии обеспечения информационной безопасности предприятия и направления их реализации.
11. Организационные меры эксплуатации системы обеспечения информационной безопасности.
12. Роль высших корпоративных органов, органов управления и акционеров в обеспечении информационной безопасности предприятия.
13. Возможности акционеров по формированию требований к информационной безопасности предприятия и контролю эффективности их выполнения.
14. Охрана объекта, охранные меры и режим охраны: сущность и содержание.
15. Содержание организации и осуществления охраны; неотложные меры руководства по защите персонала.
16. Сущность и принципы организации внутриобъектового режима.
17. Функциональные зоны внутриобъектового режима: методика разграничения и обособления .
18. Сущность и основы классификации средств охраны предприятия.
19. Сущность, содержание и принципы организации пропускного режима.
20. Контрольно-пропускной пункт: задачи, оборудование и организация дежурства.

21. Порядок осуществления пропускного режима.

22. Противопожарная защита: сущность, основы организации и средства.

23. Содержание основных документов организации противопожарной защиты.

24. Охрана конфиденциальных документов и имущества при транспортировке.

25. Требования и перечень мер по обеспечению безопасности в местах проведения закрытых и массовых мероприятий.

26. Обеспечение информационной безопасности совещаний и заседаний по конфиденциальным вопросам в ходе их подготовки.

27. Требования к помещению для проведения совещаний и заседаний по конфиденциальным вопросам.

28. Основные организационные меры по исключению закладок разведывательных электронных устройств.

29. Профилактическая работа с участниками совещаний и заседаний по конфиденциальным вопросам в интересах обеспечения информационной безопасности.

30. Обеспечение информационной безопасности совещаний и заседаний по конфиденциальным вопросам в ходе их проведения.

31. Понятие о персонале и психологических факторах воздействия на него как источниках угроз информационной безопасности.

32. Роль управления персоналом в обеспечении информационной безопасности предприятия, содержание функций управления персоналом, направления и методы работы с персоналом.

33. Особенности приема сотрудников на работу, связанную с конфиденциальной информацией.

34. Работа с кандидатами на замещение должностей, связанных с обработкой конфиденциальной информации.

35. Разрешительная система предприятия, обучение и увольнение персонала, связанного с конфиденциальной информацией.

36. Мониторинг осведомленности персонала о тайнах работодателя.

37. Факторы угроз информационной безопасности через СМИ и рекламу.

38. Основные приемы психологического воздействия через СМИ.

39. Типы манипулятивной рекламы и техника формирования доверия к коммуникатору в рекламных материалах и СМИ как фактор угроз информационной безопасности личности.

40. Роль и задачи органов управления в формировании условий обеспечения информационной безопасности при работе со СМИ и в рекламно-выставочной деятельности.

41. Задачи пресс-службы по обеспечению информационной безопасности деятельности предприятия.

42. Меры, исключающие открытое опубликование информации с ограниченным доступом в плане мероприятий по защите конфиденциальной информации на предприятии.

43. Формы и особенности работы со СМИ руководителя предприятия и его пресс-службы.

44. Направления защиты информации предприятия в ходе публикаторской деятельности.

45. Основы защиты информации предприятия в рекламно-выставочной деятельности.

46. Деятельность по обеспечению сервисов и содержание управления инцидентами.

47. Принципы эффективной политики реагирования на инциденты информационной безопасности.

48. Содержание основных инцидентов в обеспечении информационной безопасности согласно требованиям ГОСТ Р ИСО/МЭК ТО 18044-2007.

49. Содержание политики менеджмента инцидентов информационной безопасности согласно ГОСТ Р ИСО/МЭК ТО 18044-2007.

50. Содержание политики, ресурсы и инструменты расследования инцидентов информационной безопасности согласно ГОСТ Р ИСО/МЭК ТО 18044-2007.

51. Модели команды реагирования на инциденты и по расследованию инцидентов информационной безопасности.

52. Уровни организационных ролей и распределения ответственности в ходе эскалации реагирования на инциденты информационной безопасности.

53. Содержание процессов управления инцидентами, контроля проблем и ошибок согласно модели ITIL (Information Technology Infrastructure Library).

54. Содержание и виды эскалации проблемы в обеспечении информационной безопасности согласно модели ITIL.

55. Содержание понятия «риски» и технологии их анализа в интересах защиты информации.

56. Понятие качественной и количественной оценки рисков, шкалы и критерии измерения.

57. Комплексная оценка рисков безопасности и ее основные этапы. Особенности применения инструментальных средств оценки рисков на примере программного комплекса MSAT (Microsoft Security Assessment Tool).

58. Критерии оценки уровня информационной безопасности предприятия. Методика оценки рисков OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation).

59. Оценка текущего состояния информационной безопасности компании. Модели оценки угроз безопасности КСЗИ.

60. Сущность правовой нормы. Информационно-правовые нормы и их классификация.

61. Технико-правовые нормы в обеспечении информационной безопасности. Основы технического регулирования.

62. Роль и место информационного права в базовых звеньях отраслей права РФ.

63. Структура и направленность правовых мер обеспечения информационной безопасности.

64.Информация в правовой системе. Юридические особенности и свойства информации.

65. Сущность, назначение информационного права и содержание информационных отношений.

66. Методы правового регулирования и принципы информационного права.

67. Условия субъектности в информационном праве. Субъекты и объекты правоотношений в информационной сфере.

68. Система и нормы информационного права.

69. Сущность, содержание и социально-правовая структура информационных отношений. Правонарушения в информационной сфере.

70. Информационные правоотношения, возникающие при производстве, передаче и распространении информации, информационных ресурсов, продуктов и услуг.

71. Информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения.

72. Информационные правоотношения, возникающие при создании и применении средств и механизмов информационной безопасности.

73. Характеристики информационного общества, отражаемые Окинавской хартией глобального информационного общества 2000 г.

74. Структура Окинавской хартии глобального информационного общества 2000 г. Окинавская хартия о вхождении государств в информационное общество.

75. Сущность и Соглашения о сотрудничестве государств - участников СНГ в области обеспечения информационной безопасности и его основные положения.

76. Проблемы принятия международных конвенций по информационной безопасности. Предложения РФ в области совершенствования международной информационной безопасности.

77. Назначение базовых международных стандартов обеспечения информационной безопасности ISO/IEC 27001, 27002, 27003, 27004, 27007, 27011.

78. Акты отрасли информационного законодательства РФ и отрасли законодательства, акты которых включают отдельные информационно-правовые нормы.

79. «Стратегия обеспечения национальной безопасности РФ до 2020 г.» об информационной безопасности.

80. Сущность, предназначение и структура Доктрины информационной безопасности РФ.

81. Доктрина информационной безопасности РФ о национальных интересах России в информационной сфере и составляющих их достижения.

82 Задачи и методы обеспечения информационной безопасности в Доктрине информационной безопасности РФ.

83. Исходная концептуальная схема обеспечения информационной безопасности организаций Банковской системы РФ.

84. Сущность, роль и место политик безопасности в деятельности предприятия. Стратегии и политика обеспечения информационной безопасности согласно требованиям ГОСТ Р ИСО/МЭК 13335-1-2006.

85. Структура, исходные данные и уровни документирования требований политики информационной безопасности согласно требованиям ГОСТ Р ИСО/МЭК 17799-2005.

86. Сущность, цели, задачи лицензирования отдельных видов деятельности, основные принципы и полномочия органов, уполномоченных для ведения лицензионной деятельности.

87. Перечень видов деятельности, лицензируемых в интересах защиты государственной тайны и лицензионные требования.

88. Лицензирование деятельности по технической защите конфиденциальной информации, лицензионные требования, предъявляемые к соискателю лицензии и лицензиату.

89. Сущность, место и роль сертификации в техническом регулировании согласно требованиям ФЗ № 184 от 27 декабря 2002 г. Предмет технического регулирования.

90. Содержание сертификации в техническом регулировании согласно требованиям ФЗ № 184 от 27 декабря 2002 г.

91. Информация как объект правовых отношений.

92. Содержание, объект, виды и право интеллектуальной собственности.

93. Объекты институтов права интеллектуальной собственности.

94. Содержание интеллектуальных прав и отношения исключительного права на интеллектуальную собственность. Распоряжение исключительным правом.

95. Сущность и содержание, а также виды и исполнение лицензионного договора.

96. Нарушения и защита личных неимущественных и исключительных прав на интеллектуальную собственность.

97. Сущность, функции, источники и субъекты авторского и смежного права.

98. Объекты авторского права.

99. Содержание авторских прав.

100. Договоры, заключаемые автором произведения.

101. Защита авторских и смежных прав.

102. Сущность и принципы патентного права.

103. Объекты патентных прав.

104. Субъекты патентного права.

105. Порядок выдачи патента на изобретение и отказ в его выдаче.

106. Защита прав патентообладателей.

107. Правовая охрана фирменных наименований.

108. Правовая охрана товарных знаков, знаков обслуживания и наименований мест происхождения товаров.

109. Основы государственного лицензирования деятельности, связанной с защитой государственной тайны.

110. Сущность, субъекты и организация деятельности СМИ.

111. Отношения средств массовой информации с гражданами и организациями.

112. Права и обязанности журналиста.

113. Ответственность за нарушение законодательства о средствах массовой информации.

114. Сущность, особенности и субъекты компьютерных преступлений.

115. Классификация компьютерных преступлений.

116. Компьютер как объект и орудие преступления.

117. Содержание уголовно-правовой характеристики компьютерных преступлений.

118. Особенности расследования компьютерных преступлений.

119. Ответственность за компьютерные правонарушения.

120. Электросвязь в РФ и субъекты права в области связи.

121. Основы государственного регулирования в области связи.

122. Регулирование использования радиочастотного спектра.

123. Условия лицензирования и сертификации в области связи.

124. Защита и ограничение прав пользователей услугами связи, обязанности операторов связи.

Критерии и показатели оценки:

Оценивание знаний студентов по дисциплине «Организационное и правовое обеспечение информационной безопасности» осуществляется в ходе текущего контроля успеваемости и промежуточной аттестации в балльно-рейтинговой системе МГЛИ.

Оценка знаний студентов включает:

1. Результаты текущего контроля успеваемости – до 15 баллов.

2. Оценку работы студента в течение семестра – до 10 баллов.

3. Оценка знаний студента на экзамене – 40-60 баллов.

Критерии оценивания ответов на вопросы дифференцированного зачета.

Для получения 19-20 баллов за ответ на вопрос студент должен:

1. Исчерпывающе владеть терминологическим аппаратом по теме, ее метаязыком; видеть системные связи объекта с общим контекстом дисциплины и смежными вопросами.

2. Иметь системное представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть методикой анализа объекта, видеть связь теоретических аспектов темы с прикладными исследованиями.

4. Уметь выстраивать связные научные формулировки ответа с опорой на базовые понятия и категории; проявлять необходимую степень самостоятельности в представлении темы в ее внутренней логике.

Для получения 20-24 баллов студент должен:

1. В достаточной мере владеть терминологическим аппаратом по теме; видеть системные связи объекта со смежными вопросами.

2. Иметь общее представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть основными принципами методики анализа объекта, видеть связь теоретических аспектов темы с прикладными исследованиями.

4. Уметь выстраивать связные научные формулировки с опорой на базовые понятия и категории; проявлять необходимую степень самостоятельности в представлении темы в ее внутренней логике.

Для получения 15-18 баллов студент должен:

1. В достаточной мере владеть терминологическим аппаратом по теме, не допуская серьезных ошибок понятийного характера.

2. Иметь минимально необходимое представление об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Владеть основными принципами методики анализа объекта, не допуская серьезных ошибок при характеристике объекта.

4. Уметь выстраивать научные формулировки с опорой на базовые понятия и категории.

Менее 15 баллов выставляется студенту в том случае, если он:

1. Не владеет терминологическим аппаратом по теме.

2. Не имеет представлений об истории вопроса и эволюции методологических представлений о теме и объекте.

3. Не владеет принципами анализа объекта.

4. Не умеет выстраивать связные научные формулировки.