

«Организационное и правовое обеспечение информационной безопасности»

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОЛЖСКИЙ ИНСТИТУТ ЭКОНОМИКИ, ПЕДАГОГИКИ И ПРАВА»

Факультет информационной безопасности и права

Фонд оценочных средств

по дисциплине

«Организационное и правовое обеспечение информационной безопасности»

Направление подготовки:

09.03.03 Прикладная информатика

Направленность (профиль) образовательной программы:

Прикладная информатика в юриспруденции

Уровень высшего образования:

бакалавриат

Квалификация выпускника:

«бакалавр»

Волжский, 2026 г.

Содержание

1	Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы, описание показателей, критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания.....	3
2	Методические материалы и типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.....	7
2.1	Типовые контрольные задания, используемые для проведения входного контроля	7
2.2	Типовые контрольные задания, используемые для промежуточной аттестации по дисциплине.....	9
2.2.1	Примерный перечень вопросов к зачету	9
2.2.2	Примерное задание на зачет	11
2.3	Методические материалы и типовые контрольные задания, используемые для текущего контроля по дисциплине	11
2.3.1	Методические материалы, используемые для текущего контроля знаний по дисциплине	11
2.3.2	Вопросы, выносимые на самостоятельное изучение	12
2.3.3	Задания для самостоятельной работы	12
2.3.4	Тесты по дисциплине	13
2.3.5	Типовые задания.....	15
2.3.6	Задания для контрольной работы	16
2.3.7	Методика проведения лекции-дискуссии	18
2.3.8	Методика проведения интерактивного решения задач	18
3	Методические материалы, определяющие процедуры оценивания знаний, умений, навыков по дисциплине.....	19

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы, описание показателей, критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Перечень компетенций	Показатели оценивания компетенций	Критерии оценивания компетенций	Этапы формирования компетенций	Шкала оценивания
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	- знает основные принципы правового регулирования ИБ в РФ; - умеет анализировать правовые коллизии в сфере ИБ; - владеет методиками выбора оптимальных решений при ограничениях ресурсов.	- имеет базовые знания нормативно-правовой базы ИБ; - умеет на основе типовых примеров анализировать правовые коллизии; - владеет навыками выбора решений в стандартных ситуациях.	Начальный	удовлетворительно (60–74 балла)
	- знает основные принципы правового регулирования ИБ в РФ; - умеет анализировать правовые коллизии в сфере ИБ; - владеет методиками выбора оптимальных решений при ограничениях ресурсов.	- знает нормативно-правовую базу ИБ; - умеет анализировать правовые коллизии в нестандартных ситуациях; - владеет навыками самостоятельного выбора оптимальных решений с учетом ресурсных ограничений.	Основной	хорошо (75–89 баллов)
	- знает основные принципы правового регулирования ИБ в РФ; - умеет анализировать правовые коллизии в сфере ИБ; - владеет методиками выбора	- знает нормативно-правовую базу ИБ на уровне эксперта; - умеет анализировать сложные правовые коллизии; - владеет опытом принятия оптимальных решений в условиях неопределенности и	Завершающий	отлично (90–100 баллов)

	оптимальных решений при ограничениях ресурсов.	ограниченных ресурсов.		
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	- знает нормативные требования к распределению ответственности за ИБ; - умеет выстраивать взаимодействие с коллегами при решении задач ИБ; - владеет навыками деловой коммуникации в профессиональной среде.	- имеет базовые знания о распределении ответственности за ИБ; - умеет на основе типовых примеров выстраивать взаимодействие; - владеет базовыми навыками деловой коммуникации.	Начальный	удовлетворительно (60–74 балла)
	- знает нормативные требования к распределению ответственности за ИБ; - умеет выстраивать взаимодействие с коллегами при решении задач ИБ; - владеет навыками деловой коммуникации в профессиональной среде.	- знает требования к распределению ответственности за ИБ; - умеет выстраивать эффективное взаимодействие в нестандартных ситуациях; - владеет навыками самостоятельной деловой коммуникации.	Основной	хорошо (75–89 баллов)
	- знает нормативные требования к распределению ответственности за ИБ; - умеет выстраивать взаимодействие с коллегами при решении задач ИБ; - владеет навыками деловой коммуникации в профессиональной среде.	- знает требования к распределению ответственности за ИБ на уровне эксперта; - умеет разрешать конфликтные ситуации при распределении ответственности; - владеет опытом эффективной командной работы при проведении аудитов ИБ.	Завершающий	отлично (90–100 баллов)
ПК-6. Способен квалифицированно проводить юридическую экспертизу	- знает правовые требования к лицензированию ПО; - умеет проводить юридическую экспертизу ПО; - владеет методиками анализа	- имеет базовые знания требований к лицензированию ПО; - умеет на основе типовых примеров проводить экспертизу; - владеет базовыми навыками анализа	Начальный	удовлетворительно (60–74 балла)

программного обеспечения в профессиональной деятельности, обеспечивать эксплуатацию комплекса средств автоматизации технологических решений	лицензионной чистоты ПО.	лицензионной чистоты.		
	- знает правовые требования к лицензированию ПО; - умеет проводить юридическую экспертизу ПО; - владеет методиками анализа лицензионной чистоты ПО.	- знает требования к лицензированию ПО; - умеет самостоятельно проводить юридическую экспертизу; - владеет навыками самостоятельного анализа лицензионной чистоты.	Основной	хорошо (75–89 баллов)
	- знает правовые требования к лицензированию ПО; - умеет проводить юридическую экспертизу ПО; - владеет методиками анализа лицензионной чистоты ПО.	- знает требования к лицензированию ПО на уровне эксперта; - умеет проводить комплексную юридическую экспертизу; - владеет опытом взаимодействия с правообладателями ПО.	Завершающий	отлично (90–100 баллов)
ПК-7. Способен принимать решения в точном соответствии с законодательством РФ и совершать юридические действия в организации ИТ инфраструктуры и управлении информационной безопасностью	- знает правовые основы организации ИТ-инфраструктуры; - умеет принимать управленческие решения в области ИБ с учетом законодательства; - владеет техниками документального оформления решений в области ИБ.	- имеет базовые знания правовых основ ИТ-инфраструктуры; - умеет на основе типовых примеров принимать решения; - владеет базовыми навыками документального оформления.	Начальный	удовлетворительно (60–74 балла)
	- знает правовые основы организации ИТ-инфраструктуры; - умеет принимать управленческие решения в области ИБ с учетом законодательства; - владеет техниками документального оформления решений в области ИБ.	- знает правовые основы ИТ-инфраструктуры; - умеет самостоятельно принимать решения в нестандартных ситуациях; - владеет навыками самостоятельного документального оформления.	Основной	хорошо (75–89 баллов)
	- знает правовые основы	- знает правовые основы ИТ-	Завершающий	отлично (90–100)

	организации ИТ-инфраструктуры; - умеет принимать управленческие решения в области ИБ с учетом законодательства; - владеет техниками документального оформления решений в области ИБ.	инфраструктуры на уровне эксперта; - умеет принимать решения в условиях правовой неопределенности; - владеет опытом представления интересов организации при взаимодействии с контролирующими органами.		баллов)
--	--	--	--	---------

2. Методические материалы и типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

2.1. Типовые контрольные задания, используемые для проведения входного контроля

1. Что такое информационная безопасность согласно Федеральному закону «О безопасности»?

- а) Защита информации от несанкционированного доступа
- б) Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
- в) Комплекс мер по защите персональных данных
- г) Технические средства защиты информации

2. Какой федеральный закон регулирует вопросы обработки персональных данных в РФ?

- а) ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- б) ФЗ № 152-ФЗ «О персональных данных»
- в) ФЗ № 390-ФЗ «О безопасности»
- г) ФЗ № 187-ФЗ «О безопасности критической информационной инфраструктуры»

3. Что такое государственная тайна?

- а) Информация, составляющая коммерческую тайну организации
- б) Защищенная государством информация, отнесенная к государственной тайне
- в) Любая информация, ограниченная в доступе
- г) Информация о деятельности государственных органов

4. Какой орган осуществляет лицензирование деятельности в области защиты информации?

- а) Роскомнадзор
- б) ФСБ России
- в) ФСТЭК России
- г) Минцифры России

5. Что такое коммерческая тайна?

а) Информация, имеющая действительную или потенциальную коммерческую ценность

- б) Государственная тайна в коммерческих организациях
- в) Информация о финансовой деятельности организации
- г) Конфиденциальная информация о сотрудниках

6. Какой стандарт серии ISO/IEC 27000 устанавливает требования к системе менеджмента информационной безопасности?

- а) ISO/IEC 27000
- б) ISO/IEC 27001
- в) ISO/IEC 27002
- г) ISO/IEC 27005

7. Что такое риск информационной безопасности?

- а) Вероятность реализации угрозы безопасности информации
- б) Потенциальный ущерб от нарушения безопасности информации
- в) Комбинация вероятности события и его последствий
- г) Уязвимость информационной системы

8. Какой документ определяет политику информационной безопасности организации?

- а) Приказ руководителя
- б) Положение о коммерческой тайне
- в) Политика ИБ
- г) Инструкция по обработке персональных данных

9. Что такое инцидент информационной безопасности?

а) Любое событие в информационной системе
 б) Событие, которое угрожает конфиденциальности, целостности или доступности информации

- в) Вирусная атака на информационную систему
- г) Нарушение правил внутреннего распорядка

10. Какой орган осуществляет надзор за соблюдением законодательства в области персональных данных?

- а) ФСТЭК России
- б) ФСБ России
- в) Роскомнадзор
- г) Прокуратура РФ

11. Что такое лицензионная чистота программного обеспечения?

а) Отсутствие вредоносного кода в ПО
 б) Наличие у организации прав на использование ПО в соответствии с лицензионным соглашением

- в) Соответствие ПО требованиям ГОСТ
- г) Отсутствие ошибок в программном коде

12. Какой документ регламентирует порядок уведомления об обработке персональных данных?

- а) Федеральный закон № 152-ФЗ
- б) Постановление Правительства РФ № 781
- в) Приказ Роскомнадзора от 05.09.2013 № 516
- г) Все перечисленные документы

13. Что такое аудит информационной безопасности?

- а) Проверка технических средств защиты информации
- б) Систематический независимый процесс получения и оценки доказательств
- в) Внутренняя проверка соблюдения политик ИБ
- г) Проверка лицензионной чистоты ПО

14. Какой документ определяет ответственность за нарушение требований законодательства в области ИБ?

- а) Уголовный кодекс РФ
- б) Кодекс РФ об административных правонарушениях
- в) Гражданский кодекс РФ
- г) Все перечисленные документы

15. Что такое система управления информационной безопасностью (СУИБ)?

- а) Комплекс технических средств защиты информации
- б) Совокупность политик, процессов, процедур и технических средств
- в) Отдел информационной безопасности организации
- г) Программное обеспечение для мониторинга ИБ

16. Какой орган разрабатывает требования к защите информации в государственных информационных системах?

- а) ФСБ России
 - б) ФСТЭК России
 - в) Роскомнадзор
 - г) Минцифры России
17. Что такое персональные данные согласно ФЗ № 152-ФЗ?
- а) Любая информация о физическом лице
 - б) Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
 - в) Информация о трудовой деятельности физического лица
 - г) Информация, содержащаяся в трудовой книжке
18. Какой документ регламентирует порядок проведения оценки соответствия в области защиты информации?
- а) Федеральный закон № 184-ФЗ «О техническом регулировании»
 - б) Приказ ФСТЭК России от 11.02.2013 № 21
 - в) ГОСТ Р ИСО/МЭК 27001
 - г) Все перечисленные документы
19. Что такое организационные меры защиты информации?
- а) Технические средства защиты информации
 - б) Меры, реализуемые путем установления правил, процедур и ответственности
 - в) Физические средства защиты информации
 - г) Программные средства защиты информации
20. Какой документ определяет полномочия должностных лиц по обеспечению ИБ в организации?
- а) Должностная инструкция
 - б) Положение о системе управления ИБ
 - в) Приказ о назначении ответственных лиц
 - г) Все перечисленные документы

2.2. Типовые контрольные задания, используемые для промежуточной аттестации по дисциплине

2.2.1. Примерный перечень вопросов к зачету

Теоретические вопросы

1. Конституционные основы информационной безопасности в Российской Федерации.
2. Федеральный закон «О безопасности»: основные положения и полномочия органов государственной власти в сфере ИБ.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации»: классификация информации и порядок ограничения доступа.
4. Правовое регулирование государственной тайны: основные понятия, порядок отнесения информации к государственной тайне.
5. Федеральный закон «О персональных данных»: основные принципы и условия обработки персональных данных.
6. Правовое регулирование коммерческой тайны: понятие, условия отнесения информации к коммерческой тайне.
7. Ответственность за нарушение законодательства в области информационной безопасности (уголовная, административная, гражданско-правовая).
8. Международно-правовые аспекты обеспечения информационной безопасности.

9. Правовое регулирование лицензирования деятельности в области защиты информации.
10. Порядок уведомления об обработке персональных данных и ответственность операторов.
11. Стандарты серии ISO/IEC 27000 в области управления информационной безопасностью.
12. ГОСТ Р ИСО/МЭК 27001-2021: требования к системе менеджмента информационной безопасности.
13. Структура и содержание политики информационной безопасности организации.
14. Локальные нормативные акты по информационной безопасности: виды, содержание, порядок разработки.
15. Организационная структура обеспечения информационной безопасности в организации.
16. Методология оценки рисков информационной безопасности: основные этапы и подходы.
17. Риск-ориентированный подход к управлению информационной безопасностью.
18. Организационные меры защиты информации: виды, содержание, эффективность.
19. Планирование мероприятий по снижению рисков информационной безопасности.
20. Организация аудита системы управления информационной безопасностью.

Практические вопросы

1. Проведите анализ соответствия условной организации требованиям Федерального закона «О персональных данных».
2. Разработайте проект политики информационной безопасности для организации сферы здравоохранения.
3. Проведите оценку рисков информационной безопасности для информационной системы обработки персональных данных.
4. Разработайте план мероприятий по снижению выявленных рисков ИБ с учетом экономической целесообразности.
5. Проведите юридическую экспертизу лицензионного соглашения на программное обеспечение.
6. Разработайте проект положения о коммерческой тайне для коммерческой организации.
7. Определите круг должностных лиц, ответственных за обеспечение ИБ в организации, и распределите между ними обязанности.
8. Разработайте инструкцию для сотрудников по обработке персональных данных.
9. Проанализируйте судебную практику по делам о нарушении законодательства о персональных данных.
10. Разработайте регламент доступа к информации, составляющей коммерческую тайну.
11. Определите порядок реагирования на инцидент информационной безопасности с юридической точки зрения.
12. Проведите анализ соответствия ИТ-решения требованиям законодательства РФ в области ИБ.
13. Разработайте проект уведомления об обработке персональных данных для оператора.

14. Определите меры ответственности за нарушение требований законодательства в области ИБ в конкретной ситуации.

15. Разработайте программу обучения персонала вопросам информационной безопасности.

16. Проведите анализ коллизий между требованиями различных нормативных актов в области ИБ.

17. Разработайте проект приказа руководителя об утверждении политики ИБ.

18. Определите порядок взаимодействия с контролирующими органами при проверках в сфере ИБ.

19. Проведите анализ лицензионной чистоты программного обеспечения, используемого в организации.

20. Разработайте проект отчета по результатам внутреннего аудита системы управления ИБ.

2.2.2. Примерное задание на зачет

Задание 1. Дайте развернутый ответ на вопрос: «Правовое регулирование защиты персональных данных в Российской Федерации: основные принципы, права субъектов персональных данных, обязанности операторов».

Задание 2. Разработайте проект локального нормативного акта «Положение о коммерческой тайне» для коммерческой организации, осуществляющей деятельность в сфере информационных технологий. Обоснуйте структуру и содержание документа с точки зрения требований законодательства РФ.

2.3. Методические материалы и типовые контрольные задания, используемые для текущего контроля по дисциплине

2.3.1. Методические материалы, используемые для текущего контроля знаний по дисциплине

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Контрольный опрос	Метод оценки уровня освоения компетенций на основе непосредственного или опосредованного взаимодействия преподавателя и студента	Примерный перечень вопросов к зачету, вопросы для самостоятельного изучения
Собеседование	Метод контрольного опроса в форме относительно свободного диалога на заданную тему	Примерный перечень вопросов к зачету, вопросы для самостоятельного изучения
Тестовые задания	Эмпирико-аналитическая процедура оценки уровня освоения компетенций	Тесты по дисциплине (раздел 2.3.4)
Самостоятельное решение задач	Метод приобретения навыков творческого мышления и самостоятельного решения проблем	Типовые задания (раздел 2.3.5), задания для контрольной работы (раздел 2.3.6)
Лекция-дискуссия	Оценочное средство для включения обучающихся в процесс обсуждения спорного вопроса	Методика проведения лекции-дискуссии (раздел 2.3.7)
Интерактивное	Метод модерации при решении задач под	Методика проведения

решение задач	руководством преподавателя-модератора	интерактивного решения задач (раздел 2.3.8), типовые задания
---------------	---------------------------------------	--

2.3.2. Вопросы, выносимые на самостоятельное изучение

Блок теоретических вопросов

1. Анализ Доктрины информационной безопасности Российской Федерации: основные положения и приоритеты.
2. Сравнительный анализ правового регулирования ИБ в РФ и странах ЕС (на примере GDPR).
3. Правовое регулирование критической информационной инфраструктуры РФ.
4. Международные стандарты в области ИБ: сравнительный анализ серий стандартов ISO/IEC 27000 и NIST.
5. Правовые аспекты использования облачных технологий для обработки персональных данных.
6. Ответственность руководителя организации за нарушение требований законодательства в области ИБ.
7. Правовые основы проведения аудита информационной безопасности.
8. Порядок лицензирования деятельности по разработке средств защиты информации.
9. Правовое регулирование использования биометрических персональных данных.
10. Международное сотрудничество в области обеспечения информационной безопасности.

Блок практических вопросов

1. Анализ судебной практики Верховного Суда РФ по делам о нарушении законодательства о персональных данных за последние 3 года.
2. Разработка матрицы ответственности за обеспечение ИБ в организации с численностью более 1000 человек.
3. Проведение анализа коллизий между требованиями ФЗ № 152-ФЗ и ФЗ № 187-ФЗ в части защиты персональных данных.
4. Разработка алгоритма действий при выявлении утечки персональных данных.
5. Анализ лицензионных соглашений ведущих производителей ПО (Microsoft, Oracle, SAP) на предмет соответствия требованиям законодательства РФ.
6. Разработка программы повышения осведомленности персонала в области ИБ.
7. Проведение сравнительного анализа требований ФСТЭК России и ФСБ России к защите информации.
8. Разработка регламента взаимодействия юридической службы и службы ИБ при инцидентах информационной безопасности.
9. Анализ практики привлечения к ответственности за нарушение требований законодательства в области ИБ (административные штрафы, уголовные дела).
10. Разработка проекта договора на оказание услуг по обеспечению ИБ с учетом требований законодательства РФ.

2.3.3. Задания для самостоятельной работы

1. Подготовьте аналитическую справку по изменениям в законодательстве РФ в области ИБ за последние 2 года.

2. Разработайте проект инструкции для сотрудников по предотвращению фишинговых атак с учетом требований законодательства.
3. Проведите анализ соответствия условной информационной системы требованиям Приказа ФСТЭК России № 21.
4. Подготовьте реферат на тему: «Правовые аспекты использования искусственного интеллекта в системах обеспечения ИБ».
5. Разработайте проект регламента доступа к информации, составляющей государственную тайну, для организации с лицензией ФСБ России.
6. Проведите сравнительный анализ требований к защите персональных данных в РФ и КНР.
7. Подготовьте проект приказа об утверждении плана мероприятий по снижению рисков ИБ на основе проведенной оценки.
8. Разработайте чек-лист для проверки лицензионной чистоты программного обеспечения.
9. Подготовьте проект отчета по результатам внутреннего аудита системы управления ИБ.
10. Разработайте проект программы обучения персонала вопросам правового обеспечения ИБ.

2.3.4. Тесты по дисциплине

Тест 1. Правовые основы информационной безопасности

1. Что является высшим нормативным правовым актом в системе законодательства РФ в области ИБ?
 - а) Федеральный закон «О безопасности»
 - б) Конституция РФ
 - в) Доктрина информационной безопасности РФ
 - г) Указ Президента РФ
2. Какой орган осуществляет координацию деятельности в области обеспечения ИБ?
 - а) Совет Безопасности РФ
 - б) Минцифры России
 - в) ФСБ России
 - г) ФСТЭК России
3. Что такое информация согласно ФЗ № 149-ФЗ?
 - а) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах
 - б) Любые сведения независимо от формы их представления
 - в) Данные, представленные в электронной форме
 - г) Сведения, составляющие государственную тайну
4. Какой вид информации не может быть отнесен к информации, доступ к которой ограничен?
 - а) Государственная тайна
 - б) Информация о состоянии здоровья гражданина
 - в) Информация о деятельности государственных органов
 - г) Коммерческая тайна
5. Какой орган утверждает перечень сведений, составляющих государственную тайну?
 - а) Президент РФ
 - б) Правительство РФ

- в) Федеральное Собрание РФ
 - г) Совет Безопасности РФ
6. Какой документ определяет порядок допуска граждан к государственной тайне?
- а) Федеральный закон «О государственной тайне»
 - б) Постановление Правительства РФ № 1375
 - в) Указ Президента РФ № 403
 - г) Приказ ФСБ России
7. Что такое персональные данные специальных категорий?
- а) Персональные данные, касающиеся расовой, национальной принадлежности
 - б) Персональные данные руководителей организаций
 - в) Персональные данные, обрабатываемые в информационных системах персональных данных
 - г) Персональные данные, составляющие государственную тайну
8. Какой орган осуществляет лицензирование деятельности по защите государственной тайны?
- а) ФСБ России
 - б) ФСТЭК России
 - в) Роскомнадзор
 - г) Минцифры России
9. Какой срок хранения персональных данных установлен законодательством РФ?
- а) 3 года
 - б) 5 лет
 - в) Не более срока, необходимого для целей обработки
 - г) 10 лет
10. Какой документ регламентирует порядок уничтожения носителей персональных данных?
- а) Федеральный закон № 152-ФЗ
 - б) Постановление Правительства РФ № 781
 - в) ГОСТ Р 53718-2009
 - г) Приказ Роскомнадзора
- Тест 2. Организационное обеспечение информационной безопасности
1. Какой международный стандарт устанавливает требования к системе менеджмента информационной безопасности?
- а) ISO/IEC 27000
 - б) ISO/IEC 27001
 - в) ISO/IEC 27002
 - г) ISO/IEC 27005
2. Что является основным документом системы управления ИБ организации?
- а) Политика ИБ
 - б) Регламент доступа к информации
 - в) Инструкция по обработке персональных данных
 - г) Приказ о назначении ответственных лиц
3. Какой орган в организации несет персональную ответственность за обеспечение ИБ?
- а) Руководитель организации
 - б) Начальник отдела ИБ
 - в) Главный инженер
 - г) Юрист

4. Что такое риск информационной безопасности?
 - а) Вероятность реализации угрозы
 - б) Потенциальный ущерб
 - в) Комбинация вероятности и последствий
 - г) Уязвимость информационной системы
5. Какой этап оценки рисков ИБ предполагает определение стоимости активов?
 - а) Идентификация активов
 - б) Идентификация угроз
 - в) Идентификация уязвимостей
 - г) Анализ последствий
6. Какой документ определяет порядок реагирования на инциденты ИБ?
 - а) Политика ИБ
 - б) Регламент реагирования на инциденты
 - в) Инструкция по обработке персональных данных
 - г) План мероприятий по снижению рисков
7. Что такое внутренний аудит системы управления ИБ?
 - а) Проверка, проводимая внешней организацией
 - б) Проверка, проводимая сотрудниками организации
 - в) Проверка, проводимая контролирующими органами
 - г) Проверка технических средств защиты
8. Какой документ подтверждает соответствие системы управления ИБ требованиям стандарта?
 - а) Акт проверки
 - б) Сертификат соответствия
 - в) Заключение аудитора
 - г) Приказ руководителя
9. Какой принцип управления ИБ предполагает распределение прав и обязанностей между сотрудниками?
 - а) Принцип минимальных привилегий
 - б) Принцип разделения обязанностей
 - в) Принцип защиты в глубину
 - г) Принцип экономической целесообразности
10. Что такое план непрерывности бизнеса в контексте ИБ?
 - а) План развития бизнеса организации
 - б) Документ, определяющий действия при нарушении ИБ
 - в) Документ, обеспечивающий продолжение критически важных операций при инцидентах ИБ
 - г) План обучения персонала

2.3.5. Типовые задания

Задача 1: Разработка политики информационной безопасности

Описание задачи: Разработайте проект политики информационной безопасности для коммерческой организации, осуществляющей деятельность в сфере электронной коммерции и обрабатывающей персональные данные клиентов.

Задание:

1. Определите цели и задачи политики ИБ с учетом специфики деятельности организации.

2. Разработайте структуру политики ИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001-2021.

3. Определите организационные меры защиты информации для ключевых процессов организации.

4. Разработайте раздел политики, регламентирующий обработку персональных данных в соответствии с ФЗ № 152-ФЗ.

5. Определите порядок мониторинга и анализа эффективности реализации политики ИБ.

Критерии оценки:

1. Соответствие структуры и содержания политики требованиям законодательства РФ и международных стандартов.

2. Учет специфики деятельности организации в сфере электронной коммерции.

3. Полнота охвата ключевых аспектов обеспечения ИБ.

4. Практическая применимость разработанных положений.

5. Логичность и последовательность изложения материала.

Задача 2: Проведение оценки рисков информационной безопасности

Описание задачи: Проведите оценку рисков информационной безопасности для информационной системы обработки персональных данных клиентов организации.

Задание:

1. Проведите идентификацию информационных активов системы и определите их ценность.

2. Определите актуальные угрозы безопасности информации для данной системы.

3. Выявите уязвимости информационной системы и оцените их критичность.

4. Проведите анализ рисков с использованием матрицы вероятность/воздействие.

5. Разработайте план мероприятий по снижению высоких и средних рисков с учетом экономической целесообразности.

Критерии оценки:

1. Полнота идентификации активов, угроз и уязвимостей.

2. Корректность оценки вероятности и воздействия рисков.

3. Обоснованность выбора мероприятий по снижению рисков.

4. Учет экономической целесообразности при планировании мероприятий.

5. Документальное оформление результатов оценки рисков.

2.3.6. Задания для контрольной работы

2.3.6.1. Задание к теоретической части контрольной работы

Задание 1: Юридическая экспертиза программного обеспечения

Описание: Проведите юридическую экспертизу лицензионного соглашения на использование программного обеспечения «1С:Предприятие 8» в государственной организации.

Задание:

1. Проанализируйте лицензионное соглашение на предмет соответствия требованиям законодательства РФ.

2. Выявите потенциальные правовые риски при использовании ПО в государственной организации.

3. Разработайте рекомендации по устранению выявленных нарушений и минимизации правовых рисков.

4. Подготовьте заключение юридической экспертизы в соответствии с требованиями нормативных актов.

Критерии оценки:

1. Полнота анализа лицензионного соглашения.
2. Корректность выявления правовых рисков.
3. Обоснованность разработанных рекомендаций.
4. Соответствие оформления заключения требованиям законодательства.

Задание 2: Разработка системы документального обеспечения ИБ

Описание: Разработайте комплект локальных нормативных актов по информационной безопасности для коммерческой организации с численностью 250 человек.

Задание:

1. Определите перечень необходимых локальных нормативных актов в соответствии с требованиями законодательства РФ.
2. Разработайте структуру и содержание ключевых документов: политики ИБ, положения о коммерческой тайне, инструкции по обработке персональных данных.
3. Обеспечьте взаимную увязку разработанных документов.
4. Разработайте регламент вступления документов в силу и порядок их актуализации.

Критерии оценки:

1. Полнота перечня локальных нормативных актов.
2. Соответствие содержания документов требованиям законодательства РФ.
3. Логичность и последовательность структуры документов.
4. Практическая применимость разработанных документов.

2.3.6.2. Задание к практической части контрольной работы

Задача 1: Анализ инцидента информационной безопасности

Описание: В организации произошла утечка персональных данных 500 клиентов в результате несанкционированного доступа к базе данных.

Задание:

1. Определите правовые последствия инцидента в соответствии с ФЗ № 152-ФЗ.
2. Разработайте алгоритм действий руководителя организации при выявлении инцидента.
3. Определите порядок уведомления субъектов персональных данных и Роскомнадзора.
4. Разработайте план мероприятий по предотвращению подобных инцидентов в будущем.

Задача 2: Разработка регламента доступа к информации

Описание: Разработайте регламент доступа к информации, составляющей коммерческую тайну, для отдела разработки программного обеспечения.

Задание:

1. Определите перечень информации, относящейся к коммерческой тайне в отделе разработки.
2. Разработайте матрицу ролей и полномочий для сотрудников отдела.
3. Определите технические и организационные меры контроля доступа.
4. Разработайте процедуру отзыва доступа при увольнении сотрудника.

2.3.7. Методика проведения лекции-дискуссии

Цель: Достижение определенного мнения по обсуждаемой проблеме путем осознания участниками своих мнений, суждений, оценок по теме дискуссии; уточнения взаимных позиций в споре; выработки уважительного отношения к другому мнению.

Задачи:

- развитие умений анализировать проблему или проблемную ситуацию в сфере правового регулирования ИБ;
- поиск и разработка перспективных идей по совершенствованию законодательства в области ИБ;
- развитие способности продуцировать множество решений правовых коллизий;
- нахождение оптимального решения среди нескольких альтернатив.

Методика проведения:

- назначение секретаря лекции-дискуссии, его инструктаж по выполняемым функциям;
- объявление критериев оценки;
- свободный обмен мнениями в промежутках между логически оформленными разделами сообщения учебного материала;
- подведение итогов дискуссии и оценка участников дискуссии по материалам, подготовленным секретарем, переход к информационной лекции.

Критерии оценки: секретарь лекции-дискуссии – 0,5–1,5 балла; участие в дискуссии – 0,5–1 балл.

2.3.8. Методика проведения интерактивного решения задач

Цель: Проверка навыков решения профессиональных задач в области правового и организационного обеспечения ИБ и развитие мыслительных операций обучающихся, направленных на достижение результатов при решении профессиональных задач.

Задачи:

1. проверка навыков применения обучающимися ранее усвоенных знаний при решении профессиональных задач в области ИБ;
2. формирование навыков совместной деятельности подчиненных (обучающихся) и руководителя (преподавателя);
3. овладение обучающимися знаниями и общими принципами решения проблемных профессиональных задач;
4. развитие навыков активной интеллектуальной деятельности;
5. развитие коммуникативных навыков (навыков общения);
6. развитие навыков обучающихся по выработке собственной позиции по ходу решения профессиональных задач.

Методика проведения интерактивного решения задач:

Первый этап «подготовка проекта решения задач». Преподавателем разрабатывается проект хода решения задачи с началом или фрагментами решения.

Второй этап «организационный»:

1. объявление темы и цели решения задачи;
2. назначение секретаря и его инструктаж по выполняемым функциям;
3. объявление критериев оценки.

Третий этап «интеллектуальный»:

1. объявление условий решения задач;

2. индивидуальное решение задачи обучающимися, исходя из собственного мнения;
3. высказывание обучающимися мнений по ходу решения задач;
4. обсуждение результатов и методики индивидуального решения задач обучающимися и принятие плана верного хода решения.

Четвертый этап «подведение итогов решения задачи»:

1. формулирование вывода решения задачи обучающимися;
2. подведение итога интерактивного решения задачи преподавателем;
3. оценка преподавателем обучающихся по материалам, подготовленным секретарем.

Критерии оценки: секретарь – 1 балл; участие в решении задач – 1–3 балла.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков по дисциплине

Балльно-рейтинговая система оценки успеваемости по дисциплине

В целях оперативного контроля уровня усвоения материала учебной дисциплины и стимулирования активной учебной деятельности студентов (очной формы обучения) используется балльно-рейтинговая система оценки успеваемости. В соответствии с этой системой оценки студенту в ходе изучения дисциплины предоставляется возможность набрать не менее 60 баллов за текущую работу в семестре и до 40 баллов на зачете (итоговый контроль). Результирующая оценка по дисциплине складывается из суммы баллов текущего и итогового контроля.

К зачету допускаются студенты, посетившие все лекции и практические занятия, прошедшие промежуточную аттестацию, с рейтингом не менее 30 баллов.

Баллы за текущую работу в семестре по дисциплине складываются из следующих видов деятельности студента:

Балльно-рейтинговая система по дисциплине «Организационное и правовое обеспечение информационной безопасности»

Виды контроля	Максимальная сумма баллов на выполнение одного вида задания	Всего возможных за семестр работ	Итого максимальная сумма баллов
Присутствие на лекционных и практических занятиях	0,25	48	12
Работа на практических занятиях	1,0	8	8
Интерактивные занятия	2,0	4	8
СРС, в т.ч.:			32
написание конспектов нормативных актов	0,5	10	5
подготовка рефератов по актуальным вопросам ИБ	2,0	5	10
выступление с докладом на практическом занятии	1,5	4	6
выполнение типовых заданий	2,0	4	8

написание эссе по правовым коллизиям в сфере ИБ	1,0	3	3
Контроль СРС (тестирование, решение кейсов)	2,0	4	8
Итого за семестр	—	—	60
Зачет	40,0	1	40
Итого по дисциплине	—	—	100

Текущий контроль по лекционному материалу проводит лектор. Текущий контроль по практическим занятиям проводит преподаватель, проводивший эти занятия.

Балльно-рейтинговая система предусматривает поощрение студентов за работу в семестре проставлением «премиальных» баллов.

Нормы выставления дополнительных баллов по дисциплине «Организационное и правовое обеспечение информационной безопасности»

Виды работ	Максимальная сумма баллов
Подготовка и публикация научной статьи по тематике дисциплины	5
Участие в студенческой научной конференции по вопросам ИБ	3
Разработка практических рекомендаций для реальной организации	5
Итого	10

Шкала итоговой оценки

Количество баллов	Оценка
90–100	«отлично»
75–89	«хорошо»
60–74	«удовлетворительно»
0–59	«не зачтено»