

**Федеральное государственное бюджетное учреждение науки
Институт машиноведения им. А.А. Благонравова
Российской академии наук
(ИМАШ РАН)**

УТВЕРЖДАЮ
Заместитель директора по вопросам
подготовки кадров высшей
квалификации ИМАШ РАН
к.ф.-м.н. Жданов Э.Р.
« 01 » _____ 2026 года
М.П.



**Комплект оценочных материалов
по дисциплине «Информационная безопасность»**

Направление подготовки:	02.04.03 Математическое обеспечение и администрирование информационных систем
Профиль подготовки:	Искусственный интеллект и интеллектуальная обработка данных
Квалификация:	Магистр
Форма обучения	Очная

Содержание

1. Общие положения.....	3
2. Результаты освоения дисциплины, подлежащие проверке.....	3
3. Контроль и оценка освоения учебной дисциплины.....	4
4. Оценочные материалы для проведения текущего контроля успеваемости.....	4
5. Оценочные материалы для проведения промежуточной аттестации.....	11

1. Общие положения

Комплект оценочных материалов (далее - ОМ) предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу дисциплины «Информационная безопасность».

ОМ включают контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации в форме экзамен.

ОМ разработаны на основании:

- основной профессиональной образовательной программы по направлению подготовки 02.04.03 Математическое обеспечение и администрирование информационных систем;

- рабочей программы дисциплины «Информационная безопасность».

2. Результаты освоения дисциплины, подлежащие проверке

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями

ПК-2	Управление работами системных аналитиков
ПК-2.1	Разработка методик выполнения работ подчиненными системными аналитиками на всем жизненном цикле
ПК-2.2	Контроль и координация работ, выполняемых подчиненными системными аналитиками

Код индикатора компетенции	Планируемые результаты обучения по дисциплине
ПК-2.1	<i>Знать:</i> - нормативно-правовые акты РФ и международные стандарты в области ИБ. - методологию Secure SDLC и принципы интеграции ИБ в процессы разработки. - специфику угроз ИБ для систем искусственного интеллекта и методы их классификации. <i>Уметь:</i> - формулировать требования к информационной безопасности в составе технических заданий. - разрабатывать регламенты и инструкции для подчиненных аналитиков по выполнению работ с учетом требований ИБ. - оценивать риски ИБ на этапах анализа и проектирования системы. <i>Иметь практический опыт:</i> - разработки методики выполнения работ по анализу защищенности системы на этапе сбора требований. - создания регламента для подчиненных по верификации реализации мер защиты в проектной документации.
ПК-2.2	<i>Знать:</i> - методы и инструменты контроля качества выполнения работ с точки зрения информационной безопасности. - принципы координации действий команды при выявлении инцидентов или уязвимостей. - порядок документирования результатов контроля и отчетности перед руководством. <i>Уметь:</i> - осуществлять контроль за соблюдением утвержденных методик и регламентов по ИБ при выполнении работ подчиненными. - координировать действия команды по устранению выявленных уязвимостей в установленные сроки. - проводить аудит промежуточных результатов работы на соответствие требованиям безопасности. <i>Иметь практический опыт:</i>

	- координации работы группы аналитиков при проведении моделирования угроз для сложной ИИ-системы. - подготовки отчета о результатах контроля выполнения работ с указанием выявленных отклонений от стандартов ИБ.
--	--

3. Контроль и оценка освоения учебной дисциплины

Элемент учебной дисциплины	Текущий контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые идк	Форма контроля	Проверяемые идк
Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	Отчет по лабораторному практикуму	ПК-2.1		
Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	Реферат	ПК-2.1		
Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации	Отчет по лабораторному практикуму	ПК-2.1		
Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации	Отчет по лабораторному практикуму	ПК-2.1 ПК-2.2		
Тема 4. Защита информации в информационных система	Отчет по лабораторному практикуму	ПК-2.1 ПК-2.2		
Тема 4. Защита информации в информационных система	Эссе	ПК-2.1		
			Экзамен	ПК-2.1 ПК-2.2

4. Оценочные материалы для проведения текущего контроля успеваемости

Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Лабораторный практикум
20-16 – работа выполнена в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, сделаны необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы; 15-11 – работа выполнена в срок, самостоятельно, правильно поняты и использованы соответствующие формулы, правильно определены соответствующие спецификации, использована требуемая информация, правильно выполнены требуемые расчеты, правильно выбраны совместимые комплектующие, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 10-6 – работа выполнена в срок, в основном самостоятельно, использованы соответствующие

формулы; определены соответствующие спецификации, имеются ошибки в расчетах; выбраны совместимые комплектующие необходимые, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 5-1 – обучающийся подготовил работу самостоятельно или не завершил в срок, описание спецификации содержит незначительные ошибки, выводы и ответы на вопросы отсутствуют.
Реферат
10-8 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 7-5 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 4-1 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения.
Эссе
10-8 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 7-5 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 4-1 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения.

Порядок начисления баллов

Если студент набрал достаточное количество баллов ТКУ по дисциплине (более 70 баллов) в течение семестра, он может отказаться от сдачи экзамена, и результат будет выставлен автоматически по его согласию.

Типовые контрольные задания и иные материалы, необходимые для процедуры оценивания знаний, умений, навыков и(или) опыта деятельности

Типовые задания для лабораторных практикумов

Лабораторный практикум № 1. Общие проблемы безопасности. Основные положения теории информационной безопасности

Задание 1.

1. Придумайте, компанию, для которой вы будете разрабатывать нормативное и административно-организационное обеспечение информационной безопасности. Это может быть:

- вымышленная компания;
 - компания, где вы работаете;
 - компания, по которой планируете выполнять дипломный проект;
 - компания, где вы проходили практику;
 - компания, описание и данные по которой вы использовали в рамках другого курса;
2. Приведите краткое описание компании:
- название, организационно-правовая форма, учредители
 - краткая история компании (год основания, основные этапы развития)
 - сфера деятельности
 - миссия
 - количество сотрудников
 - организационная структура (представить в виде рисунка)
 - способы ведения бизнеса
 - основные конкуренты и конкурентная стратегия
 - основные поставщики и потребители (клиенты)
 - цели компании на ближайшие год (не менее 5 целей), три года (не менее 5 целей),

пять лет (не менее 5 целей).

Задание 2.

Определить основные активы компании, и занести данные в соответствующую таблицу. Количество активов каждого вида определяется особенностями компании и должно соответствовать информационным потокам компании, а также используемым программным и техническим средствам для их обработки.

Вид деятельности	Наименование актива	Форма представления	Владелец актива	Критерии определения стоимости	Размерность оценки	
					Количественная	Качественная
Информационные активы						
Активы программного обеспечения						
Физические активы						

Задание 3.

Провести ранжирование активов по пятибалльной шкале по степени их значимости для компании, выявить наиболее ценные активы. Данные представить в виде таблицы.

Наименование актива	Ценность актива (ранг)

Задание 4.

Разработка политики информационной безопасности

1. Ознакомьтесь с прилагаемыми нормативными документами для разработки политики информационной безопасности (ИБ), а также учебным фрагментом политики ИБ компании «Ин Техно» (в фрагменте представлена общая политика ИБ без указания конкретных деталей, сроков, ответственных лиц и так далее).

2. Разработайте проект политики ИБ для вашей организации. При этом следует акцентировать внимание на следующих аспектах:

- цели политики ИБ;
- основные принципы;
- на кого будет распространяться эта политика;
- выделение групп пользователей
- выделение основных видов информационных ресурсов;
- определение уровней доступа (атрибутов безопасности) к информации:
 - открыто (О)
 - конфиденциально (К)
 - секретно (С),
 - совершенно секретно (СС)
 - особая важность (ОВ)
- определение политики в отношении паролей, в частности:
 - повторяемость / неповторяемость паролей
 - количество паролей, хранимое системой
 - максимальный срок действия пароля
 - минимальный срок действия пароля
 - минимальная длина пароля
 - соответствие требованиям сложности
 - параметры блокировки учетных записей (пороговое значение блокировки, время блокировки, сброс счетчика блокировки)
- определение политики в отношении доступа к ресурсам сети Internet, в частности:
 - использование доступа к сети Internet в личных целях

- ведение «белого» или «черного» списка сайтов
- временной интервал доступа сети Internet
- объем скачиваемой и загруженной информации
- возможности использования ресурсов сети Internet различными группами пользователей
- использование почтовых и иных сервисов
- контроль за использованием ресурсов сети Internet
- что разрешено, а что запрещено различным группам пользователей;
- рекомендации для пользователей.

Политика ИБ должна отвечать на следующие вопросы

1. Насколько возможно использование Интернет в личных целях?
2. Ограничивать ли работу в Интернет в нерабочее время?
3. Как решаются вопросы конфиденциальности корпоративной информации?
4. Какое место занимают вопросы безопасности в политике ИБ?
5. На кого распространяется эта политика?
6. Какие права оставляет за собой организация?
7. Какие юридические аспекты необходимо учитывать?
8. Прочие вопросы.

Лабораторный практикум № 2. Нормативно-правовые аспекты информационной безопасности и защиты информации

Задание 1.

Провести оценку уязвимости активов. Данные представить в виде таблицы (либо таблиц, т.к. удобнее сформировать отдельную таблицу для каждого типа активов). С примерами типовых уязвимостей можно ознакомиться в приложении D стандарта ГОСТ Р ИСО/МЭК 27005-2010.

Активы					
Группа уязвимостей и содержание уязвимости	Актив 1	Актив 2	Актив 3	...	Актив N
Аппаратные средства					
Программные средства					
Сеть					
Персонал					
Место функционирования организации					
Организация					

Задание 2.

Определить перечень информационных активов, обязательное ограничение доступа, к которым регламентируется действующим законодательством РФ, а также отнесенных компанией к коммерческой тайне. Данные представить в виде таблицы.

№ п/п	Наименование сведений	Гриф конфиденциальности	Нормативный документ, реквизиты, №№ статей

Лабораторный практикум № 3. Административно-организационные аспекты информационной безопасности и защиты информации

Задание 1. Проведите оценку угроз активам. Данные представить в виде таблицы.

Группа угроз/ Содержание угроз	Актив 1	Актив 2	Актив 3	...	Актив N
1. Угрозы, обусловленные преднамеренными действиями					
2. Угрозы, обусловленные случайными действиями					
3. Угрозы, обусловленные естественными причинами (природные, техногенные факторы)					

Задание 2. Проведите оценку рисков информационной безопасности. Данные представьте в виде таблиц оценки «штрафных баллов» и результатов оценки рисков ИБ (таблица 3.2).

Оценивание рисков проводится экспертным путем на основе анализа ценности активов, возможности применения угроз и использования уязвимостей, определенных в предыдущих заданиях. Для оценивания используется таблица с заранее предопределенными «штрафными баллами» для каждой комбинации ценности активов, уровня угроз и уязвимостей.

Пример оценки уровня угроз и уязвимостей («штрафных баллов»)

	Уровни угрозы	Низкая			Средняя			Высокая		
	Уровни уязвимости	Н	С	В	Н	С	В	Н	С	В
Ценность активов	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

В случае определения уровня уязвимости из результатов аудита или самооценки для различных процессов и при наличии экспертных оценок уровня соответствующих угроз и ценности активов можно получить меру риска ИБ для каждого процесса.

Результаты оценки рисков информационной безопасности

Риск	Актив	Ранг риска

Лабораторный практикум № 4. Защита информации в информационных системах

На основе данных, полученных при выполнении предыдущих заданий и произвольных данных потерях из-за инцидентов информационной безопасности, и затратах

на систему ИБ и провести расчет показателей эффективности системы ИБ.

Задание 1. Рассчитать величину потерь ДО модернизации системы ИБ. Данные представить в таблице 4.1.

Величины потерь (рисков) для критичных информационных ресурсов до/после внедрения/модернизации системы защиты информации

Актив	Угроза	Величина потерь (тыс.руб.)

Задание 2. Рассчитать объем разового и постоянного ресурса, выделяемого на защиту информации. Данные представить в таблицах Ресурс, выделяемый на защиту информации, может иметь разовый и постоянный характер. Разовый ресурс расходуется на закупку, установку и наладку дорогостоящей техники, постоянный - на заработную плату сотрудникам службы безопасности и поддержание определенного уровня безопасности, прежде всего, путем эксплуатации технических средств и контроля эффективности защиты.

Содержание и объем разового ресурса, выделяемого на защиту информации

Организационные мероприятия				
п/п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час)	Стоимость, всего (тыс.руб.)
Стоимость проведения организационных мероприятий, всего				
Мероприятия инженерно-технической защиты				
№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
Стоимость проведения мероприятий инженерно-технической защиты				
Объем разового ресурса, выделяемого на защиту информации				

Содержание и объем постоянного ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п/п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час)	Стоимость, всего (тыс.руб.)
Стоимость проведения организационных мероприятий, всего				
Мероприятия инженерно-технической защиты				
№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
Стоимость проведения мероприятий инженерно-технической защиты				
Объем постоянного ресурса, выделяемого на защиту информации				

Задание 3.

Рассчитать величину потерь ПОСЛЕ модернизации системы ИБ. Данные представить в таблице 4.1.

Задание 4.

Рассчитать показатели экономической эффективности системы ИБ.

Пусть

R_{Σ} - суммарное значение ресурса, выделенного на защиту информации за год

$K_{\text{ср}}$ – реальные среднегодовые потери из-за инцидентов информационной безопасности (потери ДО модернизации)

$R_{\text{прогн}}$ – прогнозируемые потери после модернизации системы ИБ (потери ПОСЛЕ модернизации)

Тогда срок окупаемости затрат на обеспечение ИБ составит:

$$T_{\text{ок}} = R_{\Sigma} / (R_{\text{ср}} - R_{\text{прогн}})$$

Задание 5.

Обменяйтесь выполненным практикумом с вашим одногруппником. Проведите условный анализ выполнения основных задач по обеспечению безопасности на основе полученных данных.

Анализ выполнения основных задач по обеспечению информационной безопасности

Основные задачи по обеспечению информационной безопасности	Степень выполнения

Дополнительно опишите ваши замечания по полученным данным, в частности по оценке информационных активов, рисков, угроз, политики ИБ и так далее.

Примерные темы рефератов:

1. Сравнительный анализ сетевых сканеров.
2. Сравнительный анализ программных межсетевых экранов.
3. Сравнительный анализ аппаратных межсетевых экранов.
4. Сравнительный анализ систем обнаружения атак или вторжений.
5. Международные стандарты в сфере безопасности сетей.
6. Российское законодательство по информационной безопасности и безопасности сетей.
7. Международное законодательство по информационной безопасности и безопасности сетей.
8. Сравнительный анализ производителей аппаратных средств обнаружения и отражения сетевых атак.
9. Сравнительный анализ разработчиков программных средств обнаружения и отражения сетевых атак.
10. Сравнительный анализ комплексных программных средств обеспечения сетевой безопасности.
11. Сравнительный анализ комплексных аппаратных средств обеспечения сетевой безопасности.
12. Комплекс программных решений в области информационной безопасности компании Infowatch.
13. Комплекс программных решений в области информационной безопасности Лаборатории Касперского.
14. Комплекс программных решений в области информационной безопасности

компании Symantec.

15. Комплекс программных решений в области информационной безопасности компании SearchInform.

Примерные темы эссе:

1. Защита систем трансляции, передачи сообщений и электропитания.
2. Защита помещения от утечки акустической информации через акустоэлектрические преобразователи телефонной цепи и аппарата.
3. Акустопреобразовательные элементы с передачей информативного сигнала радиоизлучением.
4. Акустоэлектрические преобразователи, технические характеристики акустопреобразовательного канала.
5. Криптографическая защита телефонных сообщений.
6. Активные способы защиты телефонных линий.
7. Пассивные способы защиты телефонных линий.
8. Телефонная линия как канал утечки информации, индуктивный и бесконтактный съем информации с телефонной линии.
9. Комбинированные способов технической защиты телефонных линий.
10. Способы технической защиты в IP телефонии.
11. Радиозакладные устройства.
12. Сетевые закладные устройства.
13. Средства и способы обнаружения радиозакладных устройств.
14. Комплексы мониторинга технических каналов утечки информации.
15. Активное противодействие закладным радиоустройствам.
16. Акустические устройства перехвата информации.
17. Защита конфиденциальной акустической информации от несанкционированной аудио записи.
18. Портативные средства аудиозаписи, способы и средства противодействия.
19. Переносные средства аудиозаписи, способы и средства противодействия.
20. Способы и средства проверки звукоизоляции помещений.
21. Средства контроля эффективности акустической защиты.
22. Аппаратно-программные комплексы виброакустических измерений.
23. Пассивные способы защиты акустической информации.
24. Активные способы защиты акустической информации.
25. Комплексные системы защиты акустической информации.
26. Защита конфиденциальной информации от несанкционированной аудиозаписи.
27. Портативные средства видеозаписи, способы и средства противодействия.
28. Переносные средства видеозаписи, способы и средства противодействия.
29. Технические каналы утечки информации.
30. Технические средства информационной разведки и промышленного шпионажа.

5. Оценочные материалы для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме экзамена.

Экзамен представляет собой выполнение обучающимся заданий билета, включающего в себя:

Задание №1 – теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень владения обучающегося принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними.

Задание №2 – задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности.

Задания №3 – задания на проверку умений и навыков, полученных в результате освоения дисциплины.

Выполнение обучающимся заданий билета оценивается по следующей балльной шкале:

Задание 1: 0-30 баллов

Задание 2: 0-30 баллов

Задание 3: 0-40 баллов

-90 и более (отлично) – ответ правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат.

-70 и более (хорошо)– ответ в целом правильный, логически выстроен, приведены необходимые выкладки, использована профессиональная лексика. Ход решения задания правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат.

-50 и более (удовлетворительно)– ответ в основном правильный, логически выстроен, приведены не все необходимые выкладки, использована профессиональная лексика. Задания решены частично.

-менее 50 (неудовлетворительно)– ответы на теоретическую часть неправильные или неполные. Задания не решены.

Типовые задания для проведения промежуточной аттестации обучающихся

Задания 1 типа

1. Государственные органы власти, обеспечивающие защиту информации в России.
2. Основные федеральные законы в области защиты информации.
3. Технология двухфакторной аутентификации.
4. Идентификация в вычислительной системе.
5. Циклические коды.
6. Недостатки систем хеширования.
7. Способы защиты информации.
8. Стратегии защиты информации.
9. Периметр охраняемой территории.
10. «Абсолютная» система защиты.
11. Понятие информационной безопасности
12. Что такое защита информации?
13. Основные составляющие информационной безопасности
14. Что понимают под целостностью информационных ресурсов?
15. Что такое конфиденциальность?
16. Важность и сложность проблемы информационной безопасности.
17. Сущность объектно-ориентированного подхода.
18. Инкапсуляция при объектно-ориентированном подходе.
19. Наследование при объектно-ориентированном подходе
20. Полиморфизм при объектно-ориентированном подходе
21. Грани объекта при объектно-ориентированном подходе
22. Уровень детализации при объектно-ориентированном подходе.
23. Компонент и контейнер компонент.
24. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
25. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.

Задания 2 типа

Задача 1. В компании внедрена система электронного документооборота. При проверке выяснилось, что сотрудники подписывают документы простой электронной

подписью (ПЭП) без дополнительного соглашения об использовании ПЭП и без фиксации действий в журнале аудита.

Требуется: выявить нарушения, сослаться на ФЗ №63 и внутренние требования к ЭЦП, предложить меры по приведению системы в соответствие.

Задача 2. Оператор ПД обрабатывает данные 50 000 субъектов, уровень защищённости — УЗ-2. В ходе аудита обнаружено, что резервное копирование выполняется на внешний диск, который хранится в общедоступном шкафу, а журнал событий на серверах отключён.

Требуется: определить нарушения требований приказа ФСТЭК №21, оценить риски (вероятность/ущерб), предложить срочные и плановые меры.

Задача 3. В сети компании (Active Directory) 40% учётных записей имеют избыточные права: обычные сотрудники — права локальных администраторов, несколько менеджеров — права на изменение прав доступа.

Требуется: классифицировать угрозы, указать, какие модели управления доступом нарушены (RBAC/ABAC), предложить поэтапный план минимизации привилегий.

Задача 4. Компания использует облачный сервис SaaS для хранения ПД клиентов. Провайдер находится за рубежом, в договоре нет положений о месте хранения данных и порядке реагирования на инциденты.

Требуется: оценить соответствие ФЗ №152, указать обязательные условия договора с провайдером, предложить перечень контрольных вопросов для аудита провайдера.

Задача 5. В отделе кадров утерян USB-накопитель с персональными данными 120 сотрудников (ФИО, должности, зарплаты). Носитель не был зашифрован.

Требуется: классифицировать инцидент по шкале критичности, описать шаги реагирования в первые 24 часа, определить обязательства по уведомлению (сроки, кому направлять) согласно ФЗ №152 и методическим рекомендациям ФСТЭК.

Задача 6. Веб-приложение компании уязвимо к SQL-инъекциям. Разработчики утверждают, что «это не критично, потому что вход только по корпоративной учётной записи».

Требуется: опровергнуть это утверждение, привести сценарии атаки, указать меры защиты (SAST/DAST, параметризованные запросы, WAF), соотнести с OWASP Top-10.

Задача 7. В университете студенты и преподаватели используют один и тот же Wi-Fi без сегментации, гостевые устройства подключаются к той же сети, что и серверы с ПД.

Требуется: описать угрозы (перехват, MITM, заражение ботнетом), предложить архитектуру сегментации (VLAN, отдельный гостевой сегмент), указать принципы defence in depth.

Задача 8. Сотрудник службы безопасности обнаружил в логах множественные неудачные попытки входа с одного IP-адреса в течение 15 минут. Система не блокирует учётные записи после 5 попыток.

Требуется: классифицировать событие, описать план действий (изоляция, анализ, эскалация), предложить настройки политик паролей и блокировки в соответствии с приказом ФСТЭК №21.

Задача 9. В организации не ведётся инвентаризация информационных активов, нет классификации данных по уровню конфиденциальности.

Требуется: обосновать необходимость классификации, предложить шкалу уровней (например, «общедоступные», «для служебного пользования», «конфиденциальные»), описать процедуру инвентаризации и периодического пересмотра.

Задача 10. Компания передаёт ПД третьим лицам (аутсорсинг бухгалтерии) без отдельного согласия субъектов и без договора о поручении обработки.

Требуется: указать нарушения ФЗ №152, описать обязательные элементы договора о поручении, предложить форму согласия субъекта и порядок уведомления.

Задача 11. На рабочих станциях сотрудников отключены обновления ОС и антивирусы, так как «обновления мешают работе».

Требуется: оценить риски (эксплойты, шифровальщики), сослаться на требования по управлению уязвимостями, предложить процесс управления обновлениями и исключениями.

Задача 12. В компании нет плана реагирования на инциденты, сотрудники не знают, кому сообщать о подозрительных письмах.

Требуется: разработать структуру плана (PICERL), описать роли (SOC, ИТ, ИБ, руководство), предложить регламент эскалации и сценарий тренировки (tabletop-учения).

Задача 13. При приёме на работу сотрудник подписал согласие на обработку ПД, но не давал согласия на передачу данных в систему кадрового резерва, которая принадлежит холдингу.

Требуется: определить нарушение, предложить корректный порядок получения согласий и передачи данных внутри группы компаний, сослаться на принципы ФЗ №152.

Задача 14. В банке используется двухфакторная аутентификация, но SMS-коды отправляются по открытым каналам, а логи действий пользователей хранятся только 7 дней.

Требуется: выявить уязвимости, предложить более безопасные методы 2FA (push-уведомления, приложения-аутентификаторы), обосновать требования к хранению журналов аудита.

Задача 15. В ИТ-отделе есть «мастер-учётка» с правами суперпользователя, которая используется всеми администраторами без разделения ролей.

Требуется: описать риски (неотслеживаемость действий, компрометация), предложить модель разделения привилегий и контроля (разделение обязанностей, ролевая модель, РАМ-система).

Задача 16. Компания хранит резервные копии в облаке, но не шифрует данные на стороне клиента, ключи хранятся вместе с бэкапами.

Требуется: оценить угрозы (доступ третьих лиц, утечка ключей), предложить схему управления ключами (KMS, разделение ключей, ротация), соотнести с требованиями к защите ПД.

Задача 17. В организации используется устаревшая версия веб-сервера, в которой известны критические уязвимости. Руководство отказывается обновлять из-за «возможных сбоев».

Требуется: рассчитать риски (вероятность эксплуатации, ущерб репутации и штрафы), предложить поэтапную стратегию обновления (тестовые среды, окна обслуживания), обосновать необходимость.

Задача 18. В филиале компании нет выделенного сотрудника ИБ, инциденты фиксируются в Excel-файле, уведомления отправляются по почте.

Требуется: предложить минимально достаточную архитектуру мониторинга и реагирования (SIEM-лайт, чек-листы, роли), описать процесс интеграции с головным офисом и НКЦКИ.

Задача 19. При внедрении нового сервиса ПД не проводилось категорирование объекта КИИ и не оценивались угрозы.

Требуется: описать порядок категорирования по ФЗ №187, предложить этапы оценки угроз и формирования модели нарушителя, указать последствия отсутствия мер защиты.

Задача 20. В компании сотрудники используют личные мессенджеры для обсуждения рабочих вопросов и передачи файлов.

Требуется: оценить риски утечки ПД и коммерческой тайны, предложить политику использования мессенджеров, технические меры (DLP, MDM) и организационные (обучение, дисциплинарные меры).

Задания 3 типа

Задание 1. Разработайте матрицу доступа (таблица «роль × ресурс → права») для трёх ролей (администратор, менеджер, стажер) и пяти ресурсов (файловый сервер, БД ПД,

веб-портал, почта, VPN). Обоснуйте выбор прав с точки зрения принципа минимальных привилегий и требований приказа ФСТЭК №21.

Задание 2. Составьте регламент реагирования на инцидент «утечка ПД через электронную почту» по модели PICERL. Для каждого этапа укажите действия, сроки, ответственных, необходимые артефакты (журналы, скриншоты, отчёты).

Задание 3. Разработайте проект политики парольной защиты для организации с 300 сотрудниками. Включите требования к длине, сложности, периодичности смены, исключениям для сервисных учётных записей, блокировке после неудачных попыток. Сошлитесь на приказ ФСТЭК №21 и NIST SP 800-63B.

Задание 4. Подготовьте чек-лист для аудита безопасности веб-приложения (12 пунктов). Для каждого пункта укажите критерий проверки, инструмент (например, OWASP ZAP, Burp Suite), ожидаемый результат и ссылку на OWASP Top-10.

Задание 5. Разработайте схему сегментации сети для филиала (до 50 рабочих мест) с выделением сегментов: серверный, пользовательский, гостевой, DMZ. Укажите типы межсетевых экранов, правила фильтрации, требования к маршрутизации и мониторингу.

Задание 6. Составьте перечень документов СУИБ (не менее 8 наименований) для среднего предприятия. Для каждого документа укажите назначение, периодичность актуализации, ответственного и связь со стандартом ISO/IEC 27001.

Задание 7. Разработайте форму согласия на обработку ПД для онлайн-сервиса (веб-форма). Включите обязательные элементы по ФЗ №152, укажите, как технически обеспечить подтверждение волеизъявления (чек-бокс, логирование, хранение).

Задание 8. Подготовьте план резервного копирования и восстановления для ИТ-инфраструктуры (серверы, БД, почта). Укажите RPO/RTO для разных классов данных, типы бэкапов (полный, инкрементальный), места хранения, порядок тестирования восстановления.

Задание 9. Разработайте процедуру управления уязвимостями (4 этапа: выявление, оценка, устранение, контроль). Для каждого этапа укажите инструменты (сканеры, SIEM), критерии приоритизации (CVSS), сроки устранения в зависимости от критичности.

Задание 10. Создайте проект регламента использования съёмных носителей в организации. Включите классификацию носителей, требования к шифрованию, порядок учёта и выдачи, действия при утере, ответственность сотрудников.

Задание 11. Разработайте архитектуру защиты удалённого доступа (VPN, MFA, контроль устройств). Укажите протоколы, методы аутентификации, требования к конечным устройствам (антивирус, обновления), порядок мониторинга активности.

Задание 12. Подготовьте форму оценки рисков ИБ (матрица «вероятность × ущерб») для 5 типовых угроз (утечка ПД, DDoS, шифровальщик, инсайдер, сбой БД). Для каждой угрозы укажите меры снижения риска и целевое значение остаточного риска.

Задание 13. Разработайте сценарий tabletop-учения по инциденту «шифровальщик в корпоративной сети». Включите вводную, роли участников, перечень вопросов для обсуждения, критерии успеха и форму итогового отчёта.

Задание 14. Составьте проект договора о поручении обработки ПД (фрагмент) между заказчиком и аутсорсером. Включите обязательные пункты по ФЗ №152: цели, состав данных, обязанности сторон, меры защиты, порядок реагирования, ответственность, срок хранения.

Задание 15. Разработайте классификацию информационных активов для вуза (не менее 6 категорий). Для каждой категории укажите уровень конфиденциальности, допустимые способы передачи, требования к хранению и доступу.

Задание 16. Подготовьте инструкцию по безопасной разработке для команды (10 пунктов) с учётом SDLC. Включите этапы анализа требований, тестирования безопасности, приёмки, мониторинга. Сошлитесь на OWASP и принципы безопасного кодирования.

Задание 17. Разработайте схему контроля физического доступа в серверную (СКУД, видеонаблюдение, журналы). Укажите требования к зонированию (периметр, коридор, помещение), порядок выдачи пропусков, действия при ЧС.

Задание 18. Составьте план взаимодействия с НКЦКИ при инциденте ИБ. Включите критерии уведомления, формат сообщения, сроки, каналы связи, перечень внутренних действий до уведомления.

Задание 19. Разработайте регламент управления криптографическими ключами (генерация, хранение, ротация, уничтожение). Укажите типы ключей (симметричные, асимметричные), носители, требования к ролям (администратор PKI, оператор), порядок аудита.

Задание 20. Подготовьте проект политики использования личных устройств (BYOD) в компании. Включите условия допуска, требования к безопасности (шифрование, MDM, антивирус), порядок разграничения личных и корпоративных данных, ответственность сотрудника при утере устройства.