Оценочные материалы для промежуточной аттестации по дисциплине

Название дисциплины «Управление корпоративной информационной безопасностью»

Код, направление подготовки	38.03.05 Бизнес-информатика
Направленность (профиль)	Экономика предприятий и управление бизнес-процессами
Форма обучения	Очная
Кафедра-разработчик	Менеджмента и бизнеса
Выпускающая кафедра	Менеджмента и бизнеса

Требования и темы к курсовому проекту (7 семестр):

Требования к курсовым работам во вложении ПЛ-ИЗиУ-2.12.9-19 Положение о курсовых работах ИЭиУ. - Режим доступа:

http://www.surgu.ru/instituty/institut-ekonomiki-i-upravleniya/dokumenty

Темы курсовых проектов:

1. Разработка политики информационной безопасности для предприятия [отрасль по выбору]
2. Совершенствование политики информационной безопасности для предприятия [отрасль по выбору]
3. Проектирование системы управления информационной безопасности (СУИБ) для организации малого и среднего бизнеса
4. Разработка комплекта организационно-распорядительных документов по информационной безопасности для производственного предприятия
5. Анализ рисков информационной безопасности и разработка политики снижения рисков для корпоративной информационной системы
6. Оценка и управление рисками информационной безопасности методом FAIR на примере банковской организации
7. Построение модели угроз и модели нарушителя для автоматизированной системы управления технологическим процессом (АСУ ТП)
8. Разработка матрицы рисков ИБ и плана обработки рисков для логистической компании стратегии информационной безопасности компании
9. Разработка организационно-технических мер по внедрению DLP-системы на предприятие
10. Проектирование защищённой корпоративной сети
11. Проектирование системы обнаружения вторжений для предприятий среднего
12. Разработка архитектуры SIEM-системы для мониторинга событий информационной безопасности в корпоративной среде
13. Разработка проекта по созданию защищённой корпоративной сети
14. Разработка плана реагирования на инциденты информационной безопасности и Playbook для SOC компании
15. Проектирование процесса управления инцидентами информационной безопасности
16. Разработка плана обеспечения непрерывности бизнеса (BCP) и плана восстановления после катастроф (DRP)
17. Проектирование компьютерного тренажёра оператора управления событиями и инцидентами информационной безопасности
18. Разработка типового сценария применения защищённой операционной системы в корпоративной среде
19. Аудит информационной безопасности предприятия: методика проведения и разработка рекомендаций

20. Разработка системы защиты коммерческой тайны на предприятии: правовые, организационные и технические аспекты

21. Оценка защищённости веб-приложения корпоративного портала

22. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации

23. Разработка системы защиты персональных данных сотрудников в соответствии

24. Построение Zero Trust Architecture (ZTA) для распределённой корпоративной инфраструктуры

Типовые задания для контрольной работы (8 семестр):

1. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Задание 1.1. Нормативно-правовая база информационной безопасности (ИБ – далее)

Заполните сравнительную таблицу ключевых нормативных актов в сфере ИБ России:

Документ	Регулятор	Область применения	Основные требования	Ответственность за нарушение
ФЗ № 149				
ФЗ № 152				
ФЗ № 187				
Приказы ФСТЭК				
ГОСТ Р 57580.1				

После таблицы письменно ответьте (5–7 предложений):

Какой из перечисленных документов наиболее значим для коммерческой организации, работающей с персональными данными клиентов, и почему?

Задание 1.2. Стандарты серии ISO 27000

Постройте схему взаимосвязи стандартов ISO 27001, ISO 27002, ISO 27005 и опишите:

Назначение каждого стандарта (3–5 предложений на каждый)

Как стандарты дополняют друг друга в рамках построения СУИБ

В чём ключевое отличие ISO 27001 от ISO 27002

Справочно: ISO 27001 — основа зрелой ИБ, которую можно масштабировать, оценивать, регулярно улучшать. Стандарт применим к любой организации, независимо от размера, отрасли или уровня зрелости ИБ. Он фокусируется не на конкретных угрозах или технологиях, а на управлении рисками.

2. АНАЛИТИЧЕСКАЯ - УПРАВЛЕНИЕ РИСКАМИ ИБ

Задание 2.1. Выбор объекта защиты

Выберите реальную организацию или условную компанию из одной из отраслей:

Банк

Производство

Медицина

Ритейл

Госорган

Опишите:

- Профиль организации (масштаб, ИТ-инфраструктура, характер обрабатываемых данных)
- Ключевые информационные активы (минимум 5)
- Законодательные требования к ИБ, применимые к данной организации

Задание 2.2. Модель угроз и нарушителя

Для выбранной организации разработайте:

А) Модель нарушителя (минимум 4 типа):

Тип нарушителя	Категория (внутр./внешн.)	Мотивация	Уровень квалификации	Потенциальный ущерб

Б) Перечень актуальных угроз (минимум 6):

№	Угроза	Источник	Уязвимость	Актив под угрозой	Вероятность (В/С/Н)

В) Письменный вывод (5–7 предложений): обоснуйте выбор актуальных угроз со ссылкой на отраслевую специфику.

Задание 2.3. Оценка и обработка рисков

На основе разработанной модели угроз:

А) Рассчитайте уровень риска для 4 наиболее критичных угроз по формуле:

Риск = Вероятность реализации угрозы × Величина ущерба

Используйте шкалу:

- Вероятность: Высокая (3) / Средняя (2) / Низкая (1)
- Ущерб: Критический (3) / Значительный (2) / Незначительный (1)

№	Угроза	Вер-сть	Ущерб	Уровень риска	Приоритет

Б) Разработайте план обработки рисков:

Риск	Стратегия (снижение/принятие/передача/уклонение)	Мероприятие	Ответственный	Срок	Остаточный риск

В) Обоснование (7–10 предложений): аргументируйте выбор стратегии обработки для каждого риска.

Справочно: Процесс управления рисками ИБ должен характеризоваться следующими особенностями: оценка рисков ведётся с учётом последствий для бизнеса и вероятности возникновения рисков. Осуществляются идентификация рисков, их анализ и сравнение с учётом выбранного уровня риск-толерантности

3. ПРАКТИЧЕСКИЕ ЗАДАНИЯ ДЛЯ ПОДГОТОВКИ: Разработка документации СУИБ

Задание 3.1. Политика информационной безопасности

Разработайте краткую политику ИБ для выбранной организации (объём: 2–3 страницы) со следующей обязательной структурой:

Раздел политики	**Содержание**
1. Область применения	На кого и что распространяется политика
2. Цели и принципы ИБ	CIA-триада, принцип минимальных привилегий, осведомлённость
3. Роли и ответственность	CISO, ИТ-отдел, рядовые сотрудники, руководство
4. Классификация информации	Категории (открытая / внутренняя / конфиденциальная / секретная)
5. Основные требования	Управление доступом, пароли, работа с носителями, удалённый доступ
6. Нарушения и ответственность	Виды нарушений, меры дисциплинарного воздействия
7. Пересмотр политики	Периодичность, условия внеплановой актуализации

Справочно: Внедрение СУИБ обеспечивает систематизацию процессов обеспечения информационной безопасности, расстановку приоритетов компании в сфере ИБ и управление ИБ в рамках единой корпоративной политики.

Задание 3.2. Gap-анализ и план внедрения СУИБ

Проведите упрощённый gap-анализ по 5 ключевым разделам ISO 27001

Раздел ISO 27001	**Требование**	**Текущее состояние (AS-IS)**	**Целевое состояние (TO-BE)**	**Gap**	**Приоритет**
5. Лидерство	Поддержка руководства,				

	политика ИБ				
6. Планирование	Оценка рисков, цели ИБ				
7. Поддержка	Ресурсы, осведомлённость, документация				
8. Функционирование	Управление активами, контроль доступа				
9. Оценка результатов	Мониторинг, внутренний аудит				

На основе gap-анализа разработайте план первоочередных мероприятий (горизонт — 6 месяцев):

Мероприятие	**Раздел ISO 27001**	**Ответственный**	**Ресурсы**	**Срок**	**Ожидаемый результат**
Внедрение СУИБ включает в себя оценку рисков, разработку стратегии информационной безопасности и политик безопасности, обучение персонала, а также постоянное совершенствование системы менеджмента. [Внедрение СУИБ (ISO/IEC 27001)					

Типовые вопросы к зачету (7 семестр):

1. Понятие информационной безопасности: триада CIA (конфиденциальность, целостность, доступность). Расширенные модели (CIAAN, Parkerian Hexad).
2. Угрозы безопасности информации, понятие политики безопасности и их типы. Оценка рисков ИБ и вероятности реализации угроз.
3. Классификация угроз ИБ: случайные и преднамеренные, внутренние и внешние. Понятие актуальной угрозы по методике ФСТЭК.
4. Информационная безопасность как профессиональная практическая область: методы предотвращения несанкционированного доступа, чтения, изменения, искажения и уничтожения информации. blog.rosdiplom.ru
5. Нормативно-правовое регулирование информационной безопасности в России: ФЗ-149 «Об информации», ФЗ-152 «О персональных данных», ФЗ-187 «О безопасности КИИ». Роль ФСТЭК и ФСБ.
6. Система управления 1. Понятие информационной безопасности: триада CIA (конфиденциальность, целостность, доступность). Расширенные модели (CIAAN, Parkerian Hexad).
2. Угрозы безопасности информации, понятие политики безопасности и их типы. Оценка рисков ИБ и вероятности реализации угроз. hse.ru
3. Классификация угроз ИБ: случайные и преднамеренные, внутренние и внешние. Понятие актуальной угрозы по методике ФСТЭК.
4. Информационная безопасность как профессиональная практическая область: методы предотвращения несанкционированного доступа, чтения, изменения, искажения и уничтожения информации. blog.rosdiplom.ru
5. Нормативно-правовое регулирование информационной безопасности в России. Роль ФСТЭК и ФСБ.
6. Система управления информационной безопасности (СУИБ): модель СУИБ и частный менеджмент. Разработка политики безопасности организации, её основные принципы. hse.ru
7. Стандарт ISO/IEC 27001: структура, требования, приложение A (114 мер защиты). Процесс сертификации.
8. Стандарт ISO/IEC 27005: методология управления рисками информационной безопасности. Этапы и документация.
9. Практика применения требований стандарта ISO 27001: формирование политики информационной безопасности, комплексная система защиты информации на предприятии. itm.ranepa.ru
10. Фреймворк NIST Cybersecurity Framework: функции (Identify, Protect, Detect, Respond, Recover), профили, уровни зрелости.
11. MITRE ATT&CK: назначение, структура матрицы, применение для анализа угроз и выстраивания защиты.
12. Российские стандарты информационной безопасности: ГОСТ Р 57580.1-2017 (финансовая отрасль), методические документы ФСТЭК. Требования к КИИ.
13. Концепция управления рисками информационной безопасности: идентификация активов, угроз, уязвимостей. Расчёт уровня риска.
14. Моделирование угроз и управление рисками информационной безопасности: планирование деятельности по обеспечению информационной безопасности, организация деятельности по обнаружению, предупреждению и ликвидации последствий компьютерных атак. ib.bmstu.ru
15. Методология FAIR (Factor Analysis of Information Risk): модель, количественная оценка, применение.
16. Экономика информационной безопасности: понятие ROSI (Return on Security Investment), методики расчёта, обоснование бюджета на информационной безопасности перед руководством.
17. Стратегии обработки рисков ИБ: принятие, снижение, передача (страхование), уклонение. Остаточный риск.
18. Управление персоналом ИБ-подразделения. Внутренние угрозы. Психологические основы обеспечения безопасности фирмы. itm.ranepa.ru

19. Роль CISO (Chief Information Security Officer): функции, зоны ответственности, место в корпоративной иерархии.

20. Политика информационной безопасности: структура документа, процесс разработки, утверждения и актуализации.

21. Управление доступом: модели разграничения доступа (DAC, MAC, RBAC, ABAC), принцип минимальных привилегий, системы IdAM.

22. Стратегия безопасности как часть стратегии компании: регуляторные и риск-ориентированные подходы, ответственность топ-менеджеров. sberuniversity.ru

Типовые вопросы к экзамену (8 семестр):

1. Понятие информационной безопасности: триада CIA (конфиденциальность, целостность, доступность). Расширенные модели (CIAAN, Parkerian Hexad).
2. Угрозы безопасности информации, понятие политики безопасности и их типы. Оценка рисков ИБ и вероятности реализации угроз.
3. Классификация угроз ИБ: случайные и преднамеренные, внутренние и внешние. Понятие актуальной угрозы по методике ФСТЭК.
4. Информационная безопасность как профессиональная практическая область: методы предотвращения несанкционированного доступа, чтения, изменения, искажения и уничтожения информации. blog.rosdiplom.ru
5. Нормативно-правовое регулирование информационной безопасности в России: ФЗ-149 «Об информации», ФЗ-152 «О персональных данных», ФЗ-187 «О безопасности КИИ». Роль ФСТЭК и ФСБ.
6. Система управления 1. Понятие информационной безопасности: триада CIA (конфиденциальность, целостность, доступность). Расширенные модели (CIAAN, Parkerian Hexad).
2. Угрозы безопасности информации, понятие политики безопасности и их типы. Оценка рисков ИБ и вероятности реализации угроз. hse.ru
3. Классификация угроз ИБ: случайные и преднамеренные, внутренние и внешние. Понятие актуальной угрозы по методике ФСТЭК.
4. Информационная безопасность как профессиональная практическая область: методы предотвращения несанкционированного доступа, чтения, изменения, искажения и уничтожения информации. blog.rosdiplom.ru
5. Нормативно-правовое регулирование информационной безопасности в России. Роль ФСТЭК и ФСБ.
6. Система управления информационной безопасности (СУИБ): модель СУИБ и частный менеджмент. Разработка политики безопасности организации, её основные принципы. hse.ru
7. Стандарт ISO/IEC 27001: структура, требования, приложение A (114 мер защиты). Процесс сертификации.
8. Стандарт ISO/IEC 27005: методология управления рисками информационной безопасности. Этапы и документация.
9. Практика применения требований стандарта ISO 27001: формирование политики информационной безопасности, комплексная система защиты информации на предприятии. itm.ranepa.ru
10. Фреймворк NIST Cybersecurity Framework: функции (Identify, Protect, Detect, Respond, Recover), профили, уровни зрелости.
11. MITRE ATT&CK: назначение, структура матрицы, применение для анализа угроз и выстраивания защиты.
12. Российские стандарты информационной безопасности: ГОСТ Р 57580.1-2017 (финансовая отрасль), методические документы ФСТЭК. Требования к КИИ.
13. Концепция управления рисками информационной безопасности: идентификация активов, угроз, уязвимостей. Расчёт уровня риска.
14. Моделирование угроз и управление рисками информационной безопасности: планирование деятельности по обеспечению информационной безопасности, организация деятельности по обнаружению, предупреждению и ликвидации последствий компьютерных атак. ib.bmstu.ru
15. Методология FAIR (Factor Analysis of Information Risk): модель, количественная оценка, применение.
16. Экономика информационной безопасности: понятие ROSI (Return on Security Investment), методики расчёта, обоснование бюджета на информационной безопасности перед руководством.
17. Стратегии обработки рисков ИБ: принятие, снижение, передача (страхование), уклонение. Остаточный риск.

18. Управление персоналом ИБ-подразделения. Внутренние угрозы. Психологические основы обеспечения безопасности фирмы. itm.ranepa.ru

19. Роль CISO (Chief Information Security Officer): функции, зоны ответственности, место в корпоративной иерархии.

20. Политика информационной безопасности: структура документа, процесс разработки, утверждения и актуализации.

21. Управление доступом: модели разграничения доступа (DAC, MAC, RBAC, ABAC), принцип минимальных привилегий, системы IdAM.

22. Стратегия безопасности как часть стратегии компании: регуляторные и риск-ориентированные подходы, ответственность топ-менеджеров. sberuniversity.ru

23. Сетевая безопасность предприятия: межсетевые экраны (Stateless/Stateful/NGFW), IDS/IPS, сегментация сети, DMZ.

24. Технические угрозы и построение процессов взаимодействия ИТ и ИБ отделов. Информационная безопасность документооборота компании.

25. DLP-системы (Data Loss Prevention): классификация, архитектура, анализируемые каналы, ключевые отечественные решения.

26. Криптографическая защита информации: алгоритмы, инфраструктура открытых ключей (PKI). Организация защиты персональных данных. itm.ranepa.ru

27. SIEM-системы: архитектура, принципы работы, правила корреляции событий, отечественные решения (MaxPatrol SIEM, RuSIEM).

28. Защита конечных точек: EDR-решения, антивирусная защита, контроль приложений, управление обновлениями (Patch Management).

29. Управление инцидентами информационной безопасности: классификация инцидентов, цели и задачи управления, процесс управления инцидентами, группа реагирования на инциденты информационной безопасности.

30. SOC (Security Operations Center): уровни (L1/L2/L3), функции, модели построения (собственный, outsourced, гибридный).

31. Планирование реагирования на инциденты: Playbook, SOAR-системы, автоматизация реагирования.

32. Цифровая криминалистика: принципы сбора доказательств, цепочка хранения улик (Chain of Custody), основные инструменты.

33. Управление непрерывностью бизнеса (BCM): стандарт ISO 22301, показатели RTO/RPO, разработка DRP.

34. Аудит информационной безопасности: виды, рекомендации по защите, лучшие практики обеспечения информационной безопасности

35. Тестирование на проникновение (Pentest): методологии (OWASP, PTES, OSSTMM), этапы, виды (Black/Gray/White Box).

36. Современные кибератаки: APT (Advanced Persistent Threat), ransomware, фишинг, атаки на цепочку поставок (Supply Chain Attack).

37. Последствия киберинцидентов для бизнеса: формирование стратегии киберустойчивости.

38. Импортозамещение в сфере информационной безопасности: российские средства защиты информации, реестр ФСТЭК, тенденции 2024–2025 гг. (СУИБ): модель СУ информационной безопасности и частный менеджмент. Разработка политики безопасности организации, её основные принципы.