Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Заполярный государственный университет им. Н. М. Федоровского»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
Анализ и моделирование бизнес процессов

Направление подготовки 09.04.03 «Прикладная информатика»
Профиль «Информационные системы и технологии в бизнесе»
Уровень образования: магистратура

Кафедра «Информационные системы и технологии»

Разработчик ФОС:
канд.техн.наук, доцент, Петров А.М. _____ Петров А.М.

Оценочные материалы по дисциплине рассмотрены и одобрены на заседании кафедры, протокол от 10.04.2026г. № 5.

Заведующий кафедрой _____ к.э.н., Беляев И.С.

Фонд оценочных средств по дисциплине Анализ и моделирование бизнес процессов для текущей/ промежуточной аттестации разработан в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности / направлению подготовки 09.04.03 Прикладная информатика на основе Рабочей программы дисциплины Анализ и моделирование бизнес процессов, утвержденной решением ученого совета от г., Положения о формировании Фонда оценочных средств по дисциплине (ФОС), Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся ЗГУ, Положения о государственной итоговой аттестации (ГИА) выпускников по образовательным программам высшего образования в ЗГУ им. Н.М. Федоровского.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1. Компетенции и индикаторы их достижения

Код и наименование компетенции	Индикаторы достижения
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Распознает и представляет процедуры критического анализа, методики анализа результатов исследования и разработки стратегий проведения исследований, организации процесса принятия решения
	УК-1.3 Оперирует методами установления причинно-следственных связей и определения наиболее значимых среди них; методиками постановки цели и определения способов ее достижения; методиками разработки стратегий действий при проблемных ситуациях
ОПК-3 Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями;	ОПК-3.1 Понимает принципы, методы и средства анализа и структурирования профессиональной информации
ОПК-7 Способен использовать методы научных исследований и математического моделирования в области проектирования и управления информационными системами;	ОПК-7.2 Выбирает и использует методы научных исследований и математического моделирования в области проектирования и управления ИС
ПК-7 Способен планировать аналитические работы в ИТ-проекте	ПК-7.3 Осуществляет обоснованный выбор методов планирования аналитических работ в ИТ-проектах в профессиональной области

ПК-8 Способен управлять процессами разработки и сопровождения требований к системам и управлять качеством систем	ПК-8.3 Оценивает эффективность управления процессами разработки и сопровождения систем, навыками разработки требований к системам и навыками управления качеством систем

Таблица 2. Паспорт фонда оценочных средств

№п/п	Контролируемые разделы(темы) дисциплины	Кодрезультатаобучения по дисциплине/ модулю	Оценочные средстватекущей		Оценочные средствапромежуточной	
			Наименование	Форма	Наименование	Форма
3 семестр						

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы.

2.1. Задания для текущего контроля успеваемости

Контрольные вопросы

1. Что такое информационная безопасность, и какие основные аспекты она включает?
2. Объясните концепцию конфиденциальности, целостности и доступности (CIA-триада).
3. Какие угрозы информационной безопасности наиболее распространены сегодня?
4. Что такое криптография, и как она используется для защиты данных?
5. Объясните разницу между симметричным и асимметричным шифрованием.
6. Какие методы аутентификации пользователей вы знаете?
7. Что такое межсетевой экран (firewall), и какова его роль в защите сети?
8. Какие существуют виды вредоносного ПО, и как они воздействуют на системы?
9. Объясните понятие "социальная инженерия" в контексте информационной безопасности.
10. Как осуществляется управление рисками в информационной безопасности?

Практические задания

1. Разработайте политику информационной безопасности для небольшой компании.
2. Проведите анализ уязвимостей в заданной системе с использованием специализированных инструментов.
3. Настройте межсетевой экран для защиты локальной сети.
4. Выполните шифрование и дешифрование данных с использованием OpenSSL.
5. Разработайте план реагирования на инциденты информационной безопасности.
6. Проведите аудит безопасности сети с использованием инструмента Nmap.
7. Настройте систему мониторинга событий безопасности (SIEM).
8. Создайте сценарий атаки социальной инженерии и предложите меры защиты от нее.
9. Разработайте план резервного копирования данных и восстановления после сбоя.
10. Проведите оценку рисков для информационных систем организации.

Вопросы для промежуточной аттестации

11. Что такое PKI (инфраструктура открытых ключей), и как она используется?
12. Объясните роль антивирусного ПО в защите информации.
13. Какие методы используются для защиты беспроводных сетей?
14. Что такое DDoS-атака, и как защититься от нее?
15. Каковы основные этапы проведения аудита информационной безопасности?

16. В чем заключается важность обновления программного обеспечения для безопасности?

17. Объясните концепцию "нулевого доверия" (Zero Trust) в контексте сетевой безопасности.

18. Какие существуют стандарты и нормативы в области информационной безопасности?

19. Как осуществляется контроль доступа к данным в корпоративной среде?

20. Какие инструменты используются для анализа сетевого трафика?

2.2 Темы письменных работ (эссе, рефераты, курсовые работы и др.)

Эссе

1. Влияние киберугроз на современный бизнес.
2. Роль криптографии в защите данных.
3. Преимущества и недостатки облачных решений с точки зрения безопасности.
4. Как социальная инженерия угрожает безопасности организаций?
5. Будущее информационной безопасности: вызовы и решения.
6. Этика в кибербезопасности: где проходит грань?
7. Влияние искусственного интеллекта на информационную безопасность.
8. Роль человеческого фактора в обеспечении безопасности.
9. Как COVID-19 изменил подходы к информационной безопасности?
10. Стандарты и нормативы в области защиты информации.

Рефераты

1. История развития систем информационной безопасности.
2. Методы защиты от DDoS-атак.
3. Сравнительный анализ антивирусных программ.
4. Использование брандмауэров в корпоративных сетях.
5. Обзор современных методов аутентификации пользователей.
6. Защита беспроводных сетей: технологии и методы.
7. Инфраструктура открытых ключей (PKI): принципы и применение.
8. Роль SIEM-систем в мониторинге безопасности.
9. Управление рисками в области информационной безопасности.
10. Обзор криптографических протоколов для защиты данных.

Курсовые работы

1. Разработка политики информационной безопасности для организации.
2. Анализ уязвимостей корпоративной сети и предложения по их устранению.
3. Проектирование системы резервного копирования и восстановления данных.
4. Настройка и тестирование межсетевого экрана для защиты сети.
5. Разработка плана реагирования на инциденты информационной безопасности.
6. Оценка эффективности антивирусного ПО в корпоративной среде.
7. Исследование методов защиты от фишинговых атак.
8. Проектирование системы контроля доступа к данным в организации.
9. Разработка стратегии управления рисками для IT-инфраструктуры компании.

1. Контрольные вопросы и задания
- Для текущего контроля:
1. Что такое информационная безопасность и её основные аспекты?
2. Объясните концепцию конфиденциальности, целостности и доступности

(CIA-триада).

3. Какие методы аутентификации пользователей вы знаете?

4. Что такое межсетевой экран и его роль в защите сети?

5. Как осуществляется управление рисками в информационной безопасности?

- Для промежуточной аттестации:
- Разработать политику информационной безопасности для компании.
- Провести анализ уязвимостей в заданной системе.
- Настроить межсетевой экран для защиты локальной сети.

2. Темы письменных работ

- Эссе:
- Влияние киберугроз на современный бизнес.
- Роль криптографии в защите данных.
- Рефераты:
- Методы защиты от DDoS-атак.
- Обзор современных методов аутентификации пользователей.
- Курсовые работы:
- Разработка политики информационной безопасности для организации.

3. Формы итогового контроля

- Защита курсового проекта (например, анализ уязвимостей и предложения по их устранению).
- Практическое задание: настройка системы мониторинга событий безопасности (SIEM).
- Устное собеседование по ключевым темам дисциплины.

4. Виды оценочных средств

- Тестирование (закрытые и открытые вопросы).
- Лабораторные работы (анализ, настройка, оптимизация систем безопасности).
- Презентации проектов или исследований.

1. Текущий контроль знаний:
- Тестирование (закрытые и открытые вопросы).
- Практические задания (анализ уязвимостей, настройка систем защиты).
- Лабораторные работы (работа с межсетевыми экранами, шифрование данных).
- Устные опросы по основным темам курса.

2. Промежуточная аттестация:
- Контрольные работы (анализ угроз, разработка политики безопасности).
- Рефераты и эссе на заданные темы.
- Мини-проекты (например, настройка системы мониторинга безопасности).

3. Итоговый контроль:
- Защита курсового проекта (анализ системы безопасности и разработка предложений по её улучшению).
- Выполнение итогового практического задания (настройка SIEM-системы или межсетевого экрана).
- Устное собеседование по ключевым темам дисциплины.

4. Дополнительные виды оценочных средств:
- Презентации проектов или исследований.
- Анализ кейсов успешного обеспечения информационной безопасности.

- Оценка портфолио выполненных лабораторных и практических работ за семестр.