МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Заведующий кафедрой ИСТ
_____ Данилов О. Ф.

«_____» _____ 20___ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

дисциплины: **Информационная безопасность и защита информации**

направление подготовки: **09.03.04 Программная инженерия**

направленность (профиль): **Разработка программно-информационных систем**

форма обучения: **очная**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2026062FC6FB7E4F1F37670D47CAB35B
Владелец: Клочков Юрий Сергеевич
Действителен: с 09.02.2024 до 04.05.2025

Фонд оценочных средств рассмотрен на заседании кафедры интеллектуальных систем и технологий для направления 09.03.04 Программная инженерия направленность (профиль) «Разработка программно-информационных систем

1. Формы аттестации по дисциплине

1.1. Форма промежуточной аттестации: *экзамен - 8 семестр.*

Способ проведения промежуточной аттестации: *экзамен в компьютерном классе.*

1.2. Формы текущей аттестации:

Таблица 1.1

№ п/п	Форма обучения
	ОФО
1	Коллоквиум
2	Защита лабораторных работ
3	Самостоятельная работа

2. Результаты обучения по дисциплине, подлежащие проверке при проведении текущей и промежуточной аттестации

Таблица 2.1

№ п/п	Структурные элементы дисциплины		Код ИДК	Оценочные средства	
	Номер раздела	Наименование раздела		Текущая аттестация	Промежуточная аттестация
1	1	Введение в информационную безопасность.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Вопросы коллоквиума. Отчет по лабораторной работы	Вопросы для подготовки к экзамену
2	2	Правовое обеспечение информационной безопасности.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Вопросы коллоквиума, Отчет по лабораторной работы	Вопросы для подготовки к экзамену
3	3	Организационное обеспечение информационной безопасности.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Вопросы коллоквиума, Отчет по лабораторной работы	Вопросы для подготовки к экзамену
4	4	Технические средства обеспечения информационной безопасности.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Вопросы коллоквиума, Отчет по лабораторной работы	Вопросы для подготовки к экзамену
5	5	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Вопросы коллоквиума, Отчет по лабораторной работы	Вопросы для подготовки к экзамену
6	6	Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Вопросы коллоквиума, Отчет по лабораторной работы	Вопросы для подготовки к экзамену
7	7	Защита от компьютерных вирусов	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Задания для самостоятельной работы Отчет по лабораторной работы	Вопросы для подготовки к экзамену
8	8	Криптографическое закрытие информации	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Задания для самостоятельной работы Отчет по лабораторной работы	Вопросы для подготовки к экзамену
9	9	Уничтожение остаточных данных	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Задания для самостоятельной работы	Вопросы для подготовки к экзамену
10	10	Защита от потери информации и отказов программно-аппаратных средств.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Задания для самостоятельной работы	Вопросы для подготовки к экзамену
11	11	Защита информационно-программного обеспечения на уровне операционных систем.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Задания для самостоятельной работы	Вопросы для подготовки к экзамену
12	12	Защита информации на уровне систем управления базами данных.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Задания для самостоятельной работы	Вопросы для подготовки к экзамену

13	13	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Задания для самостоятельной работы	Вопросы для подготовки к экзамену
14	14	Современные средства защиты информации от НСД.	З1, З2, З3, З4, У1, У2, У3, У4, В1, В2, В3 В4	Задания для самостоятельной работы	Вопросы для подготовки к экзамену

3. Фонд оценочных средств

3.1. Фонд оценочных средств, позволяющие оценить результаты обучения по дисциплине, включает в себя оценочные средства для текущей аттестации и промежуточной аттестации.

3.2. Фонд оценочных средств для текущей аттестации включает:

- контрольные вопросы и задания для подготовки к коллоквиумам – 14 шт. (Приложение 1);
- комплект заданий для выполнения самостоятельной работы – 8 шт. (Приложение 2);
- отчет по лабораторной работе – 1 шт. (Приложение 3).

3.3. Фонд оценочных средств для промежуточной аттестации включает:

- комплект вопросов и заданий для подготовки к экзамену – 25 шт. (Приложение 4).

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

Контрольные вопросы для подготовки к коллоквиумам

Раздел 1. Введение в информационную безопасность

1. Методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны; правовые и нормативные акты в области ИБ.
2. Защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.
3. Защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.
4. Методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.

Раздел 2. Правовое обеспечение информационной безопасности

5. Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Стандарты по оценке безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.
6. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.
7. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.
8. Режимы шифрования. Особенности шифрования данных в режиме реального времени.

Раздел 3. Организационное обеспечение информационной безопасности

9. Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.
10. Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога
11. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС.
12. Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.

Раздел 4. Технические средства обеспечения информационной безопасности

13. Защита в Internet и Intranet.
14. Понятие изолированной программной среды, защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.
15. Технические средства обеспечения информационной безопасности
16. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.

Раздел 5. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.

17. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.
18. Защита от компьютерных вирусов.
19. Криптографическое закрытие информации.
20. Уничтожение остаточных данных.

Раздел 6. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.

21. Защита от потери информации и отказов программно-аппаратных средств.
22. Защита информационно-программного обеспечения на уровне операционных систем.
23. Защита информации на уровне систем управления базами данных.
24. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.

Критерий оценки

за один коллоквиум

8-10 баллов - Дан развернутый ответ на вопрос с незначительными замечаниями или их отсутствием

4-7 баллов - Дан ответ на вопрос с существенными замечаниями. Ответ является неполным.

0-3 балла - Отсутствует ответ на вопрос или ответ дан не по теме вопроса

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

Комплект заданий для самостоятельной работы

Раздел 7. Защита от компьютерных вирусов
Задача 2. Выполнить кодировку шифром Виженера.

Раздел 8. Криптографическое закрытие информации
Задача 3. Выполнить кодировку методом перестановки.

Раздел 9. Уничтожение остаточных данных
Задача 4. Сделать обзор современных методов шифрования. Хеш функция. Симметричные и ассиметричные ключи.

Раздел 10. Защита от потери информации и отказов программно-аппаратных средств
Задача 5. Сделать обзор системы предотвращения вторжений.

Раздел 11. Защита информационно-программного обеспечения на уровне операционных систем
Задача 6. Сделать обзор межсетевых экранов.

Раздел 12. Защита информации на уровне систем управления базами данных.
Задача 7. Сделать обзор DOS и DDOS катак.

Раздел 13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях
Задача 8. Создать топологию сети с настройкой роутера на обнаружение атак с использованием списков доступа ACL.

Раздел 14. Современные средства защиты информации от НСД
Задача 9. Подготовить обзор современных средств защиты информации от НСД.

Критерий оценки

30-40 баллов выставляется, если обучающийся выполнил все задания самостоятельной (домашней контрольной) работы и успешно без замечаний защитил;

20-29 баллов выставляется, если обучающийся выполнил все задания самостоятельной (домашней контрольной) работы, но допустил незначительные ошибки;

10-19 баллов выставляется, если обучающимся выполнена часть заданий самостоятельной (домашней контрольной) работы и успешно их защитил;

0-9 баллов выставляется, если обучающийся выполнил меньшую часть заданий самостоятельной (домашней контрольной) работы, но не смог ответить на дополнительные вопросы.

Приложение 3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

Отчет по лабораторной работе

Результат выполнения каждой лабораторной работы должен быть оформлен в виде отчёта.

Структура отчёта:

1. Титульный лист с указанием номера работы, названия работы, номера варианта задания, ФИО обучающегося, группа, должность и ФИО проверяющего
2. Содержание отчета
3. Цель работы
4. Задание на работу, начальные условия, исходные данные
5. Ход выполнения работы с описанием каждого шага и пояснением результата, полученного на каждом шаге
6. Выводы по работе

Оценочный лист

Позиция для фиксирования параметров деятельности, описанной в отчете	**Оценка (баллы)**
Структура отчета	1
Оформление титульного листа	0,5
Содержание отчета	0,5
Цель работы	0,5
Задание на работу, начальные условия, исходные данные	0,5
Ход выполнения работы с описанием каждого шага и пояснением результата, полученного на каждом шаге	1
Выводы по работе	1

Критерии оценки отчета:

Основными критериями оценки выполненной и представленной для проверки работы являются:
1. Степень соответствия выполненного задания поставленным требованиям;
2. Структурирование и комментирование лабораторной работы;
3.Успешные ответы на контрольные вопросы.

За одну лабораторную работу

5 баллов - оформление соответствует требованиям, критерии выдержаны, защита всего перечня контрольных вопросов.
3-4 баллов - оформление соответствует требованиям, критерии выдержаны, защита только 80 % контрольных вопросов.
2 балла - оформление соответствует требованиям, критерии выдержаны, защита только 61 % контрольных вопросов.
1 - оформление не соответствует требованиям, критерии не выдержаны, нет защиты более 60% перечня контрольных вопросов.

Приложение 4

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

Комплект вопросов для подготовки к экзамену

1. Законодательные акты Российской Федерации в области информационной безопасности защиты данных: классификация и обзор.
2. Защита информации в кредитных организациях: направления и проблемы.
3. Информационные ресурсы общества и методы их защиты.
4. Руководящие документы Гостехкомиссии при Президенте России: классификация и обзор.
5. Аудит информационной безопасности предприятия.
6. Государственные и международные стандарты в области информационной безопасности защиты данных: классификация и обзор.
7. Средства авторизации доступа, отечественные разработки и их практическое использование на предприятиях: опыт и рекомендации.
8. Основы криптографии: история, методы и алгоритмы.
9. Защита информации в государственных организациях: нормирование и контроль.
10. Стеганография: исторический опыт и современные перспективы.
11. Программно-аппаратные технологии обеспечения защиты информации в сети Интернет.
12. Сложность алгоритмов криптографии: криптоанализ и направления исследований.
13. Политика информационной безопасности предприятия.
14. Классификация информации по степени защиты и нормативные акты.
15. Системы криптографической защиты информации в России: законодательство, организации инфраструктуры, использование в электронном обмене информацией.
16. Проблемы стеганоанализа и защиты информации в «открытом обществе».
17. Практические модели обеспечения защиты информации корпоративных систем.
18. Интеграция предприятий в Интернет и информационная безопасность: модели и способы защиты.
19. Комплексная система информационной безопасности предприятия: компоненты и задачи.
20. Защита информации в Интернет: направления и проблемы.
21. Защита информации в вычислительных сетях.
22. Электронная цифровая подпись, законодательство, инфраструктура.
23. Экономика информационной безопасности предприятия.
24. Обеспечение защиты информации в деловой переписке.
25. Атаки на информационные системы и способы защиты.

Критерии оценки:

91-100 баллов выставляется обучающемуся, глубоко и прочно усвоившему материал, исчерпывающе, грамотно и логически стройно его излагающего. Представлена схема (если в ответе на вопросе есть конструктивные элементы) Соответствующие знание, умения и владение сформированы полностью.

76-90 баллов выставляется обучающемуся, твердо знающему материал, грамотно и по существу излагающего его. Обучающийся не допускает существенных неточностей в ответе на вопросы. Соответствующие знание, умения и владение сформированы в целом полностью, но содержат отдельные пробелы.

61-75 баллов выставляется обучающемуся, который имеет знания только основного материала, но не усвоил его детали, допускает неточности, недостаточно правильные

формулировки, нарушения последовательности в изложении материала. Обучающийся показывает общее, но неструктурированное знание, в целом успешное, но не систематическое умение и владение соответствующих компетенций.

0-60 баллов выставляется обучающемуся, который не усвоил значительной части материала, допускает существенные ошибки. Обучающийся показывает фрагментарные знания (или их отсутствие), частично освоенное умение (или его отсутствие), фрагментарное применение навыка (или его отсутствие) соответствующих компетенций.