Фонд оценочных средств
для промежуточной аттестации
по дисциплине
Модели безопасности компьютерных систем

Направление подготовки (специальность)
10.05.01 Компьютерная безопасность

Направленность (профиль)
специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Присваиваемая квалификация
специалист по защите информации

Форма обучения
очная

Год набора 2026

Челябинск 2026 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.
Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».
Дисциплина: **Модели безопасности компьютерных систем**.
Семестр (семестры) изучения: 5 семестр.
Форма (формы) промежуточной аттестации: экзамен 5 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Модели безопасности компьютерных систем» направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	**Содержание компетенций согласно ФГОС (ОПОП ВО)**	**Индикаторы достижения компетенции согласно ОПОП**	**Перечень планируемых результатов обучения по дисциплине**
1	**2**	**3**	**4**
ОПК-8	Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	ОПК-8.1 Знает основные методы научных исследований при разработке моделей безопасности компьютерных систем. ОПК-8.2 Умеет применять методы научных исследований при проведении разработок моделей безопасности компьютерных систем. ОПК-8.3 Владеет способами моделирования безопасности компьютерных систем.	Знать: – виды и состав угроз информационной безопасности; – принципы и общие методы обеспечения информационной безопасности; – источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; – каналы и методы несанкционированного доступа к конфиденциальной информации; – состав объектов защиты информации. Уметь: – определять состав конфиденциальной информации; – определять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию; – определять возможные каналы и методы несанкционированного

			доступа; – принимать решения при выборе средств защиты информации на основе анализа угроз и рисков; – организовывать системное обеспечение защиты информации. Владеть: – навыками определения угроз информации в зависимости от среды эксплуатации продуктов информационных технологий; – навыками разработки основных политик безопасности; – критериями, условиями и принципами отнесения информации к защищаемой; – методологией построения систем защиты автоматизированных систем.
ОПК-11	Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	ОПК-11.1 Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков. ОПК-11.2 Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками. ОПК-11.3 Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	Знать: – типовые модели политик безопасности КС, политик управления доступом и информационными потоками. Уметь: – самостоятельно разрабатывать новые и дорабатывать типовые модели политик безопасности, управления доступом и информационными потоками, с учетом заданных требований. Владеть: – методами разработки моделей политик безопасности, управления доступом и информационными потоками.

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1. Виды оценочных средств

№ п/п	Код компетенции / планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1.	ОПК-8 ОПК-11	Раздел 1. Основные понятия и определения. Угрозы безопасности информации Раздел 2. Политика безопасности Раздел 3. Нормативный подход к безопасности	Лабораторная работа №1	Экзаменационные вопросы № 1 - 8
2.	ОПК-8 ОПК-11	Раздел 4. Модели компьютерных систем с дискреционным управлением доступом	Лабораторная работа №2	Экзаменационные вопросы № 9 - 10
3.	ОПК-8 ОПК-11	Раздел 5. Модели компьютерных систем с мандатным управлением доступом	Лабораторная работа №3	Экзаменационные вопросы № 11 - 12
4.	ОПК-8 ОПК-11	Раздел 6. Модели безопасности информационных потоков и изолированной программной среды	Лабораторная работа №4	Экзаменационные вопросы № 13 - 15
5.	ОПК-8 ОПК-11	Раздел 7. Модели компьютерных систем с ролевым управлением доступом Раздел 8. Развитие формальных моделей безопасности компьютерных систем	Лабораторная работа №5	Экзаменационные вопросы № 16 - 18

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

3.2. Содержание оценочных средств

3.2.1. Содержание лабораторных работ

Лабораторная работа №1

Реализовать серверную и клиентскую часть приложения, которые удовлетрояют следующим требованиям:

Сервер:

- обслуживание n клиентов одновременно (select\threads):

  при этом потоки необходимо синхронизировать, например, алгоритмом булочной

- авторизация пользователей:

  пароль должен быть зашифрован и расшифровываться на стороне сервера для авторизации

- аутентификация пользователей
- информация о логине\разлогине
- корректная поддержка отключения пользователя (в случае отключения по протоколу и нет)
- реализовать любым путем корректную передачу больших данных по сети:

  нужно учитывать, что стандартные сокеты не понимают, пришли ли все данные или нет, и recv() вернет ровно столько, сколько в буфере было на момент вызова функций -> при плохом соединении необходимо каким-то образом контролировать, пришли ли все данные или нет (протокол\единая неизменная схема передачи данных)

- организовать атомарность операций сервера:

  например, файл пользователя либо записался полностью, либо не записался вообще

- присылать ошибки пользователю на все случаи жизни, чтобы он понимал, что именно помешало выполнить его действие
- добавить поддержку опции единственной сессии:

  нельзя одновременно использовать 1 учетную запись для 2 и более экземпляров клиента

- также для юзеров при подключении должны создаваться папки, по аналогии с /home в unix

Бизнес-нагрузка сервера:

пользователь посылает команды серверу, которое обрабатываются ИСКЛЮЧИТЕЛЬНО на стороне СЕРВЕРА, то есть клиент посылает запрос, и ждет только ответ

Реализовать следующие команды для клиента:

- запись в файл: write [filename] [text] (условно)
- чтение из файла: read [file1 [file2 ...]]
- справка: help [cmd1 [cmd2 ...]]
- листинг директории: ls [dir1 [dir2 ...]]
- отключение: logout

Также есть опции для администратора, для которого должен быть реализован интерфейс на сервере:

- добавлять пользователей в систему, записывая их логин, пароль, группу
- удалять юзера по логину:

  при удалении пользователя необходимо удалять и его корневую директорию

- менять пароль юзеру
- посмотреть всех юзеров

Администратор должен иметь какие-то свои логин и пароль, проверка которых должна следовать принципам разумности:
в случае с логином клиента на сервер мы не должны говорить юзеру, что эта учетка уже активна, ибо это очевидная уязвимость категории auxiliary. В случае входа администратора пароль и логин должны проверяться одновременно, ибо иначе легко подобрать логин админа, а дальше уже и пароль

Клиент:
- реализовать удобный интерфейс для пользователя ()
- реализовать подключение к серверу
- реализовать timeout на долгих попытках достучаться до сервера
- IP-адрес и порт вводятся в клиент каждый раз либо считываются из файла конфигурации, который юзер может настроить
- реализовать показ текущей директории (либо на сервере должна быть команда pwd)
- реализовать обмен всеми данными по протоколу\единой схеме

Лабораторная работа №2

Реализовать дискреционную модель защиты:
В дискреционной модели защиты основной объект - матрица прав.
Выглядит она следующим образом:

_\|s1 |s2 |...|sN
o1|r11|r21|r.1|rN1
o2|r12|r22|r.2|rN2
..|r1.|r2.|r..|rN.
oN|r1N|r2N|r.N|rNN,

где
oN - объекты матрицы - файлы, папки и прочее,
sN - субъекты матрицы - пользователи и группы
rNM - право субъекта N на объект M.
В такой матрице удобно хранить права в виде char'a, составленного из битов прав

Требования:
Сервер:
Реализовать описанную модель защиты:
- при каждом действии пользователя сначала проверяются соотв. права на это действие:
  работает это по принципу приоритетного запрета, составим таблицу
  u+ g+ -> OK
  u- g+ -> FORB
  u+ g- -> FORB
  u- g- -> FORB

исходя из этого понятно, что любой запрет означает невозможность выполнить данное действие

если какое-то право не установлено, то это тоже необходимо принять за запрет
- хранение в памяти описанной матрицы в любом удобном виде, к которой будет происходить обращение для всех проверок
- периодическая выгрузка матрицы в файл
- при удалении пользователя\группы также должны удаляться записи из матрицы, связанные с этим пользователем

Добавить следующие команды для пользователя, обрабатываемые на сервере:
- чтение прав файла, допустим, rr [filename1 [filename2 ...]]
- изменение прав файла: chmod filename1[filename2 [...]] u|g subjectName rights

Лабораторная работа №3

Реализовать мандатную систему защиты:

Сервер:
- для пользователя создается метка, с которой он заходит на сервер:

пользователь может определять метку, с которой он заходит, например, он может зайти с меткой ниже своей, если ему угодно
- метка сессии должна определять права пользователя на сервере вместе с дискреционной моделью:

работает это по принципу приоритетного запрета, если в какой-то системе защиты есть запрет, то в итоге запрет. Сначала проверяется дискреционная система
- в случае отказа в какой либо системе пользователь должен понять, какая система ему отказала
- для каждого объекта и субъекта организовать хранение меток
- команда для просмотра текущей метки. Например: cm (current mark) -> unsigned int

Клиент:
- интерфейс ввода метки, с которой он заходит на сервер

Схема работы 2 моделей:

Client Server

read file ---------->
проверка дискреционной системы
(отправить отказ в случае запрета)
проверка мандатной системы
отказ\ответ на запрос <-

Лабораторная работа №4

Реализовать аудит в системе защиты:

Сервер:
- специальные атрибуты аудита у каждого объекта

- отдельный пользователь — администратор аудита (например, можно лишить его других прав)
- аудит разрешений и отказов доступа
- аудит устанавливается для выбранных субъектов
- команды для просмотра и редактирования атрибутов аудита
- журнал аудита, возможность его очистки

Лабораторная работа №5

Реализовать криптографическую подсистему в системе управления доступом.
Сервер:
- протокол связи сервера с клиентом (выбор этого протокола)
- выработка общего ключа
- шифрование всех передаваемых сообщений
- хранение ключей шифрования
- шифрование ключевой системной информации

Клиент:
- выработка общего ключа
- обмен сообщениями по шифрованному каналу связи

3.2.2. Вопросы к экзамену

1. Основные элементы теории компьютерной безопасности (сущность, субъект, доступ, право доступа, информационные потоки по памяти или по времени).
2. Основная аксиома. Проблема построения защищенной КС. Модели ценности информации: аддитивная модель, порядковая шкала, решетка многоуровневой безопасности.
3. Классификация угроз безопасности информации. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров КС.
4. Понятие политики безопасности. Модель нарушителя. Основные виды политик управления доступом и информационными потоками.
5. Политики дискреционного, мандатного, ролевого управления доступом, изолированной программной среды и безопасности информационных потоков. Представление политик безопасности.
6. Политики дискреционного управления доступом.
7. Классические стандарты информационной безопасности.
8. Классические стандарты информационной безопасности.
9. Модели компьютерных систем с дискреционным управлением доступом. Модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Анализ безопасности систем ХРУ. Монооперационные системы ХРУ. Алгоритмическая неразрешимость задачи проверки безопасности систем ХРУ.
10. Классическая модель распространения прав доступа Take-Grant.
11. Модели компьютерных систем с мандатным управлением доступом. Классическая модель Белла-ЛаПадулы.
12. Классическая модель Белла-ЛаПадулы.

13. Модели безопасности информационных потоков и изолированной программной среды.
14. Иерархия ролей. Механизм ограничений. Модель администрирования ролевого управления доступом. Администрирование множеств авторизованных ролей пользователей.
15. Безопасность информационных потоков. Защита от угроз конфиденциальности и целостности информации.
16. Развитие формальных моделей безопасности компьютерных систем.
17. Развитие формальных моделей безопасности компьютерных систем.
18. Проблема адекватности реализации модели безопасности в реальной КС. Развитие формальных моделей. Обзор семейства формальных моделей управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

В течении семестра проводится пять лабораторных работ, которые осуществляют срез знаний по основным понятиям, определениям и задачам.

На экзамене студент получает билет. В билете два теоретических вопроса. На написание ответа дается 1,5 часа. После этого происходит оценка ответа. Преподаватель может задавать вопросы по тексту ответа. Студент должен на них ответить.

При подведении итогов баллы за экзамен суммируются с баллами за лабораторные работы в течении семестра.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Лабораторная работа	3x5=15
2	Допуск к экзамену – 4 из 5 лаб.работ	
3	Экзамен (2 теоретических вопроса)	2x5=10
	Итого:	25

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания теоретического вопроса

Максимальный балл за ответ на теоретический вопрос – 5 баллов.

Отлично/зачтено/5 баллов	Хорошо/зачтено/ 4 балла	Удовлетворительно/зачтено/3 балла	Неудовлетворительно/не зачтено/0-2 балла
Обучающийся отлично знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся практически не допускает ошибок.	Обучающийся хорошо знает материал, умеет анализировать проблему и аргументировано изложить свою точку зрения. Обучающийся допускает незначительные ошибки.	Обучающийся знаком с материалом. Обучающийся допускает фактические ошибки.	Обучающийся не знает основных положений вопроса, не ориентируется в основных понятиях, излагает материал с трудом, с грубыми фактическими ошибками, либо отказывается от ответов на вопросы.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.2.2. Критерии оценки лабораторной работы

Отлично/зачтено/3 балла	Хорошо/зачтено/ 2 балла	Удовлетворительно/зачтено/1 балл	Неудовлетворительно/не зачтено/0 баллов
Лабораторная работа выполнена полно и правильно в соответствии с заданием, проведено и представлено полное тестирование систем и функций; технически правильным языком, даны верные ответы на контрольные вопросы.	Лабораторная работа выполнена не полностью, при выполнении лабораторной работы обучающимся допущены существенные ошибки, не весь функционал отражен в тестах.	Выполнена 1/3 лабораторной работы, допущены грубые ошибки, на большинство контрольных вопросов даны неверные ответы.	Не выполнена лабораторная работа.
Высокий уровень освоения проверяемых компетенций	Средний уровень освоения проверяемых компетенций	Базовый уровень освоения проверяемых компетенций	Недостаточный уровень освоения проверяемых компетенций

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

Промежуточная аттестация в целом выставляется по результатам лабораторных работ и ответа на экзаменационный билет, при условии сдачи хотя бы четырех из пяти лабораторных работ. Если какая-то часть не сдана, то студенту предлагаются дополнительные вопросы по этой части.

Критерий оценивания результатов экзамена:
0-15 баллов – неудовлетворительно (2);
16-17 баллов – удовлетворительно (3);
18-21 баллов – хорошо (4);
22-25 баллов – отлично (5).

Особенности проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обозначены в рабочей программе дисциплины (модуля).

Уровни сформированности компетенций определяется следующим образом:

1. Высокий уровень сформированности компетенций соответствует оценке «Отлично»:
   - предполагает формирование компетенций на высоком уровне, готовность к самостоятельной профессиональной деятельности,
   - студент способен аргументировать собственную точку зрения по дискуссионным вопросам дисциплины, решать ситуационные задачи, формулировать собственные выводы.
2. Средний уровень соответствует оценке «Хорошо»:
   - предполагает формирование компетенций на достаточном уровне,
   - студент способен давать развернутые ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Хорошо».

3. Базовый уровень соответствует оценке «Удовлетворительно»:
   - предполагает формирование компетенций на начальном уровне,
   - студент способен давать ответы на теоретические и практические вопросы дисциплины на уровне не ниже оценки «Удовлетворительно»,
   - студент способен отвечать на вопросы в закрытой форме. Количество правильных ответов – не менее 50%.
4. Низкий уровень соответствует оценке «Неудовлетворительно».

Специальность 10.05.01 Компьютерная безопасность
Специализация №6 «Информационно-аналитическая и техническая экспертиза компьютерных систем»
Фонд оценочных средств по дисциплине «Модели безопасности компьютерных систем»
2026 год набора, очная форма обучения

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

Проректор по учебной работе	утверждено 27.02.26	А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 8 от 19.02.2026

Председатель Ученого совета математического факультета	согласовано	А. С. Скорынин

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 08 от 14.02.2026

Заведующий кафедрой	согласовано	А. Н. Ручай
Автор (составитель)		А. Н. Ручай

Структура фондов оценочных средств соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от 27 сентября 2022 №573-1