Фонд оценочных средств
для промежуточной аттестации
по дисциплине
Методы и стандарты оценки защищенности 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

Челябинск 2025 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Специальность 10.05.01 Компьютерная безопасность.
Специализация № 6 «Информационно-аналитическая и техническая экспертиза компьютерных систем».
Дисциплина: **Методы и стандарты оценки защищенности компьютерных систем**.
Семестр (семестры) изучения: 10 семестр.
Форма (формы) промежуточной аттестации: экзамен 10 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины «Методы и стандарты оценки защищенности 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**
ПК-3	Способен проводить анализ безопасности компьютерных систем	ПК-3.1. Обладает знаниями о уровнях защищенности и доверия в компьютерных системах; об оценках рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; об оценках соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам. ПК-3.2. Демонстрирует умения: проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; формулировать и разрабатывать предложения по устранению выявленных уязвимостей. ПК-3.3. Имеет практический опыт	Знать: – российские и зарубежные стандарты в области информационной безопасности; – современные критерии и стандарты для анализа безопасности компьютерных систем. Уметь: – оценивать соответствие проектной и эксплуатационной документации информационной системы на соответствие стандарту в области информационной безопасности; – применять современные критерии и стандарты для анализа безопасности компьютерных систем. Владеть: – практическими навыками оценки защищенности на соответствие стандартам информационной

		(навыки): выполнение анализа уязвимости компьютерных систем.	безопасности ЦБ РФ в области информационных систем, функционирующих в финансовой сфере; – практическими навыками работы с современными критериями и стандартами для анализа безопасности компьютерных систем.

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.	ПК-3	Раздел 1. Оценка угроз информационной безопасности	Вопросы для устного опроса № 1-47. Самостоятельные работы № 1-4	Вопросы для экзамена № 1-13.
2.	ПК-3	Раздел 2. Стандарты оценки угроз информационной безопасности	Вопросы для устного опроса № 48-63. Самостоятельные работы № 5-6	Вопросы для экзамена № 14-20.

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. Вопросы для устного опроса для текущей аттестации

3. Информация.
4. Информационная система.
5. Угроза безопасноси информации.
6. Опередлние области применения оценки угроз информационной безопасности.
7. Характеристика угрозы информационной безопасности.
8. Источники угроз безопасности и их классификация.
9. Факторы, обуславливающие техногенные угрозы безопасности информации.
10. Идентификация угрозы безопасности информации в информационной системе.
11. Мониторинг и переоценка угроз безопасности информации.
12. Определение угроз безопасности информации в информационной системе.
13. Нарушитель информационной безопасности.
14. Оценка возможностей нарушителей.
15. Типы нарушителей.
16. Мотивации реализации нарушителями угроз безопасности информации в информационной системе.
17. Связи нарушителей.
18. Нарушители с базовым (низким) потенциалом.
19. Нарушители с базовым повышенным (средним) потенциалом.
20. Нарушители с высоким потенциалом.
21. Модель нарушителя по реализации угроз безопасности информации.
22. Способы реализации угроз безопасности информации.
23. Действия по реализации угроз информационной безопасности.
24. Реализация преднамеренных угроз безопасности информации.
25. Условия определения способов реализации угроз безопасности информационной системы.
26. Актуальная угроза безопасности информации.
27. Показатель актуальности угрозы.
28. Вероятность реализации угрозы.
29. Вербальные градации показателя вероятности реализации угрозы.
30. Возможность реализации угрозы безопасности информации.
31. Показатели, характеризующие проектную защищенность информационной системы.
32. Уровень проектной защищенности.
33. Уровень защищенности в ходе эксплуатации информационной системы.
34. Возможность реализации угрозы безопасности информации.
35. Исходные данные об угрозах безопасности информации.
36. Условия определения способов реализации угроз безопасности информационной системы.
37. Оценка степени возможного ущерба от реализации угрозы безопасности информации.

38. Определение актуальных угроз безопасности информации в информационной системе.
39. Потенциал нарушителя.
40. Классификация и виды нарушителей информационной безопасности.
41. Определение потенциала нарушителя.
42. Параметры экспертной оценки.
43. Техническая компетентность нарушителя.
44. Возможности нарушителя по доступу к информационной системе.
45. Оснащенность нарушителя.
46. Оценка потенциала нарушителя.
47. Модель угроз безопасности информации.
48. Структура модели нарушителя.
49. Структура модели угроз безопасности.
50. Стандарты информационной безопасности.
51. Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (1983).
52. Политика безопасности.
53. Классы безопасности.
54. Распределение функций безопасности по уровням модели OSI.
55. Стандарт ISO/IEC 15408.
56. Классы функциональных требований.
57. Международный стандарт ISO 17799.
58. Международные стандарты информационной безопасности.
59. Российские стандарты информационной безопасности.
60. Стандарты оценки защищенности.
61. Методы и стандарты оценки защищенности информационных систем в банковской сфере.
62. Minimum Security Requirements for Federal Information and Information Systems
63. Методика определения угроз безопасности информации в информационных системах.
64. Банковские стандарты информационной безопасности.
65. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.

3.2.2. Перечень самостоятельных работ

1. Разработка модели нарушителя.
2. Разработка модели угроз безопасности.
3. Сравнение методического документа "Minimum Security Requirements for Federal Information and Information Systems" с российскими аналогами.
4. Применение методики определения угроз безопасности информации в информационных системах.
5. Применение российских стандартов информационной безопасности.
6. Применение банковских стандарты информационной безопасности.

3.2.3. Перечень вопросов к экзамену

7. Источники угроз безопасности и их классификация.
8. Определение угроз безопасности информации в информационной системе.
9. Нарушитель информационной безопасности.
10. Модель нарушителя по реализации угроз безопасности информации.
11. Способы реализации угроз безопасности информации.
12. Актуальная угроза безопасности информации.
13. Определение актуальных угроз безопасности информации в информационной системе.
14. Потенциал нарушителя.
15. Классификация и виды нарушителей информационной безопасности.
16. Определение потенциала нарушителя.
17. Модель угроз безопасности информации.
18. Структура модели нарушителя.
19. Структура модели угроз безопасности.
20. Стандарты информационной безопасности.
21. Стандарты оценки защищенности.
22. Методы и стандарты оценки защищенности информационных систем в банковской сфере
23. Minimum Security Requirements for Federal Information and Information Systems
24. Методика определения угроз безопасности информации в информационных системах.
25. Российские стандарты информационной безопасности.
26. Банковские стандарты информационной безопасности.

Полные тексты самостоятельных работ и задания выложены на сетевом диске кафедры компьютерной безопасности и прикладной алгебры DC1\doc\.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Допуском до проведения экзамена являются сданные студентом самостоятельные работы в течение семестра. Экзамен проводится в два этапа. На первом студент отвечает на два вопроса. На втором студент решает практическую задачу по оценке защищенности компьютерной системы. Продолжительность – 90 минут.

Сводная таблица рейтинга успеваемости

№	Вид оценочного средства	Максимальное кол-во баллов
1	Устный опрос	2x5=10
2	Самостоятельная работа	6x5=30
3	Экзамен (теоретический вопрос)	2x15=30
4	Экзамен (практическая задача)	30
	Итого	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1. Критерии оценки устного опроса

На каждый устный опрос студенту предоставляются пять вопросов из списка по выбору преподавателя.

Максимальный балл за устный опрос – 5 баллов.

Максимальный балл за устный опрос за семестр – 10 баллов.

Характеристики ответа	Баллы	Уровень освоения проверяемых компетенций
Правильно даны все пять ответов	5	высокий
Правильно даны четыре ответа	4	средний
Правильно даны три ответа	3	
Правильно даны два ответа	2	базовый
Правильно дан один ответ	1	
Нет правильных ответов	0	недостаточный

4.2.2. Критерии оценки самостоятельной работы

Максимальный балл за самостоятельную работу – 5 баллов.

Максимальный балл за самостоятельные работы за семестр – 30 баллов.

5 баллов – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны верные

ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

4 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя продемонстрированы дополнительные действия в рамках тематики работы;

3 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод сделан самостоятельно, технически правильным языком, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

2 балла – самостоятельная работа выполнена полно и правильно в соответствии с заданием, вывод не сделан, даны не полные ответы на контрольные вопросы, по заданию преподавателя не продемонстрированы дополнительные действия в рамках тематики работы;

1 балл – при выполнении самостоятельной работы обучающимся допущены существенные ошибки по содержанию учебного материала, работа выполнена с нарушением, допущены грубые ошибки, на контрольные вопросы даны не верные ответы.

0 баллов – не выполнена самостоятельная работа.

4.2.3. Критерии оценивания теоретического вопроса экзамена

Максимальный баллы за ответ на теоретический вопрос – 15 баллов.

Максимальный баллы за ответы на зачете – 30 баллов.

Оценка	**Отлично/зачтено**	**Хорошо/зачтено**	**Удовлетворительно /зачтено**	**Неудовлетворительно/не зачтено**
Баллы	**13-15 баллов**	**9-12 баллов**	**6-8 баллов**	**0-5 баллов**
Критерии: 1. Полнота изложения теоретического материала. 2. Правильность и/или аргументированность изложения (последовательность действий) 3.Самостоятельность ответа	Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, в котором он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные	Студентом дан развернутый ответ на поставленный вопрос, в котором студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры,	Студентом дан ответ, свидетельствующий, в основном, о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить	Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, отсутствием логичности и

	примеры по проблематике поставленного вопроса.	логичность и последовательно выстраивает ответ. Однако, допускает неточность в ответе.	примеры, недостаточной логичностью и последовательность ю ответа.	последовательности. Выводы поверхностны. Студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

4.2.4. Критерии оценивания практической задачи экзамена

Максимальный баллы за практическую задачу/практическое задание – 30 баллов.

Оценка/баллы	**Отлично/зачтено/25-30 баллов**	**Хорошо/зачтено/15-24 баллов**	**Удовлетворительно/зачтено/8-14 баллов**	**Неудовлетворительно/не зачтено/0-7 балла**
Критерии: 1. Полнота изложения теоретического материала. 2. Правильность и/или аргументированность изложения (последовательность действий) 3.Самостоятельность ответа	Студентом верно определены границы оценки защищенности компьютерной системы, верно выбрана и применена методика оценки.	Студентом верно определены границы оценки защищенности компьютерной системы, выбрана и применена методика оценки с небольшими неточностями.	Студентом верно определены границы оценки защищенности компьютерной системы, не верно выбрана и применена методика оценки.	Студентом подготовлен ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области.
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации.

Для экзамена:

0 – 60 баллов – неудовлетворительно (2);

61 – 74 баллов – удовлетворительно (3);

75 – 90 баллов – хорошо (4);

91 – 100 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

Оценка	**Отлично/ зачтено**	**Хорошо/ зачтено**	**Удовлетворительно/ зачтено**	**Неудовлетворительно/ Не зачтено**
Баллы	**91-100 баллов**	**75-90 баллов**	**60-74 баллов**	**0-59 баллов**
Уровень освоения проверяемых компетенций	высокий	средний	базовый	недостаточный

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 «Методы и стандарты оценки защищенности компьютерных систем»
2025 год набора, очная форма обучения

Фонд оценочных средств дисциплины (модуля) одобрен и рекомендован:

Проректор по учебной работе	утверждено 24.02.25	А.А. Саламатов

Ученым советом математического факультета

Протокол заседания № 6 от 20.02.2025

Председатель Ученого совета математического факультета	согласовано	Е.А. Сбродова

Заседанием кафедры компьютерной безопасности и прикладной алгебры

Протокол заседания № 8 от 01.02.2025

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

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1