Фонд оценочных средств
для промежуточной аттестации
по дисциплине (модулю)
Компьютерная безопасность

Направление подготовки (специальность)
44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль)
Экономика и информатика

Присваиваемая квалификация (степень)
бакалавр

Форма обучения
очная

Год набора 2026

Челябинск, 2026 г.

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки (специальность): 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль): Экономика и информатика
Дисциплина: **Компьютерная безопасность**.
Семестр (семестры) изучения: 9 семестр.
Форма (формы) промежуточной аттестации: экзамен 9 семестр.
Используется балльно-рейтинговая система для оценивания результатов.

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

2.1. Компетенции, закреплённые за дисциплиной

Изучение дисциплины **«Компьютерная безопасность»** 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-2	Способен осваивать и использовать базовые научно-теоретические знания и практические умения по предмету в профессиональной деятельности	ПК-2.1. Реализует современные формы и методы воспитательной работы непосредственно на учебных занятиях и во внеурочной деятельности..	Знать: – содержание, сущность, закономерности, особенности изучаемых явлений и процессов, базовые теории в предметной области; – принципы, определяющие место предмета в общей картине мира; – основы данной дисциплины в объеме, необходимом для решения педагогических, научно- методических и организационно-управленческих задач. Уметь: – оценивать угрозы информационной и компьютерной безопасности в профессиональной деятельности; – формировать собственные мнения по изучаемым проблемам, аргументировать свою позицию. Владеть: – основами реализации научно-теоретических знаний в области компьютерной безопасности в профессиональной деятельности.

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-2	Раздел 1. Информационная безопасность в системе национальной безопасности Российской Федерации	Подготовка реферата по одной из предложенных тем	Теоретические вопросы к зачету
2	ПК-2	Раздел 2. Виды защищаемой информации ограниченного доступа.	Подготовка реферата по одной из предложенных тем	Теоретические вопросы к зачету
3	ПК-2	Раздел 3. Основы государственной политики Российской Федерации в области информационной безопасности	Подготовка реферата по одной из предложенных тем	Теоретические вопросы к зачету
4	ПК-2	Раздел 4. Информационное противоборство, методы и средства его осуществления	Подготовка реферата по одной из предложенных тем	Теоретические вопросы к зачету
5	ПК-2	Раздел 5. Методы и средства обеспечения информационной безопасности объектов информационной инфраструктуры	Подготовка реферата по одной из предложенных тем	Теоретические вопросы к зачету

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. Перечень вопросов к экзамену

1. Понятие национальной безопасности. Основные угрозы и критерии оценки состояния национальной безопасности России.
2. Категории персональных данных. Уровни защищенности информационной системы персональных данных (ИСПД).
3. Понятие информационной безопасности. Интересы личности, общества и государства в информационной сфере.
4. Обязанности обладателя конфиденциальной информации по ее защите.
5. Основные положения государственной политики и организационная основа обеспечения информационной безопасности РФ.
6. Требования к обеспечению безопасности ИСПД в зависимости от уровня защищенности ИСПД.
7. Угрозы информационной безопасности Российской Федерации.
8. Понятие информационной войны, цели и средства её ведения.
9. Контроль и надзор в сфере обеспечения информационной безопасности.
10. Понятие и основные свойства информации. Виды защищаемой информации.
11. Конституция РФ о правах и обязанностях граждан в информационной сфере.
12. Общие принципы и методы обеспечения информационной безопасности РФ.
13. Основные направления обеспечения информационной безопасности объектов критической информационной инфраструктуры (КИИ). Порядок категорирования объектов КИИ.
14. Состав преступления, предусмотренный статьей 274 УК РФ.
15. Задачи единой государственной системы обнаружения и предупреждения компьютерных атак на критически важную информационную инфраструктуру (Гос-СОПКА)..
16. Должностные обязанности руководителя подразделения информационной безопасности.
17. Правовой режим защиты государственной тайны. Порядок допуска к сведениям, составляющим гостайну.
18. Состав и содержание организационных и технических мер по защите ИСПД.
19. Правовой режим защиты коммерческой тайны.
20. Процедура оценки обстановки на объекте защиты.
21. Состав преступления, предусмотренный статьей 272 УК РФ.
22. Типовые и частные модели угроз безопасности ИСПД.
23. Состав преступления, предусмотренный статьей 273 УК РФ.
24. Состав и содержание организационных и технических мер по защите значимого объекта КИИ.
25. Состав преступления, предусмотренный статьей 274.1 УК РФ.
26. Этапы создания и структура службы безопасности предприятия.
27. Понятие и виды административной ответственности за нарушение требований информационной безопасности.
28. Задачи подразделения информационной безопасности предприятия.
29. Комплексная защита информации – сущность и задачи.
30. Должностные обязанности администратора безопасности АИС.
31. Компетенция ФСБ России в сфере обеспечения информационной безопасности.
32. Обязанности пользователя АИС по обеспечению информационной безопасности.
33. Понятие объекта КИИ. Порядок категорирования объектов КИИ.
34. Компетенция ФСТЭК России в сфере обеспечения информационной безопасности.
35. Обязанности оператора по защите персональных данных.
36. Классификация информационного оружия.

3.2.2. Примерный перечень тем докладов

1. Понятие национальной безопасности РФ. Роль и место информационной безопасности в системе национальной безопасности РФ.
2. Организационно-правовой режим защиты государственной тайны.
3. Организационно-правовой режим защиты коммерческой тайны.
4. Компьютерные преступления.
5. Законодательство о персональных данных.
6. Требования к защите ПД при их обработке в ИСПД.
7. Виды угроз безопасности ПД при их обработке в ИСПД.
8. Критическая информационная инфраструктура РФ.
9. Информационные войны и информационное оружие.
10. Этапы создания подразделения информационной безопасности, функциональные обязанности сотрудников.

3.2.3. Вопросы для устного опроса на практических занятиях

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы, угрозы национальной безопасности Российской Федерации.
3. Понятие информационной безопасности, основные составляющие национальных интересов в информационной сфере.
4. Факторы, способствующие повышению роли информационной безопасности в системе национальной безопасности.
5. Основные положения государственной политики и организационная основа обеспечения информационной безопасности.
6. Компетенция федеральных и региональных органов государственной власти в сфере обеспечения информационной безопасности.
7. Правовая и организационная система обеспечения информационной безопасности Челябинской области.
8. Интересы личности общества и государства в информационной сфере.
9. Характеристика основных видов угроз информационной безопасности.
10. Принципы обеспечения информационной безопасности.
11. Понятие информационной войны, цели и средства её ведения.
12. Основные компоненты информационной войны.
13. Понятие информационного оружия.
14. Классификация информационного оружия.
15. Понятие и свойства информации.
16. Виды защищаемой информации.
17. Обязанности обладателя по обеспечению защиты информации.
18. Режим конфиденциальности информации и порядок его введения, на примере режима коммерческой тайны
19. Конституция Российской Федерации о правах и обязанностях граждан в информационной сфере.
20. Структура законодательства в сфере обеспечения информационной безопасности.
21. Перечень статей УК РФ, предусматривающих уголовную ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
22. Федеральные органы, осуществляющие контрольные функции в сфере обеспечения информационной безопасности.

23. Административная ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
24. Понятие автоматизированной информационной системы.
25. Виды угроз безопасности информационных и телекоммуникационных систем.
26. Основные каналы утечки защищаемой информации.
27. Внешние источники угроз безопасности информационных систем.
28. Внутренние источники угроз безопасности информационных систем.
29. Элементы обстановки на объекте защиты, процедура оценки обстановки.
30. Критерии оценки защищенности автоматизированных информационных систем.
31. Структура службы безопасности предприятия.
32. Основные этапы создания службы безопасности предприятия.
33. Основные задачи, решаемые подразделением обеспечения информационной безопасности.
34. Обязанности руководителя подразделения информационной безопасности.
35. Обязанности системного администратора (администратора безопасности).
36. Обязанности пользователя автоматизированной информационной системы по обеспечению информационной безопасности.
37. Понятие и основные виды терроризма.
38. Роль информационных технологий в управлении критически важными объектами государства.
39. Способы совершения террористического акта в отношении объектов информационной инфраструктуры.
40. Использование террористическими организациями сети Интернет.
41. Понятие объекта, критически важного для обеспечения национальной безопасности государства, классификация критически важных объектов.
42. Угрозы уязвимости информационной инфраструктуры критически важных объектов.
43. Негативные последствия нарушения функционирования систем управления критически важных объектов.
44. Определение требований к защите информации в АСУ ТП.
45. Разработка и внедрение защиты АСУ ТП.
46. Обеспечение защиты информации в ходе эксплуатации АСУ ТП.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Допуском к экзамену является сделанный доклад на выбранную тему.
Экзамен проходит в виде теста в системе электронного обучения MOODLE.

Сводная таблица рейтинга успеваемости

№	Перечень контрольных мероприятий в семестре	Максимальное кол-во баллов
1	Экзамен	100
	Итого	100

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств.

4.2.1 Критерии оценивания теста на экзамене

Максимальный балл за тест – 100 баллов.

Отлично/ зачтено/ 91-100 баллов	Хорошо/ зачтено/ 75-90 баллов	Удовлетворительно/ зачтено/ 61-74 балла	Неудовлетворительно/ не зачтено/ 0-60 баллов
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

При подведении итогов учитываются результаты текущей аттестации:
Отлично/зачтено/91-100 баллов
Хорошо/зачтено/75-90 баллов
Удовлетворительно/зачтено/61-74 балла
Неудовлетворительно/не зачтено/0-60 баллов.

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».

Направление подготовки (специальность) 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль) Экономика и информатика
Фонд оценочных средств по дисциплине «Компьютерная безопасность»
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 факультета экономики и управления

Протокол заседания № 11 от 24.02.2026

Председатель Ученого совета факультета экономики и управления	согласовано	А. А. Егорова

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