

Министерство науки и высшего образования Российской Федерации

ЧИТИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕН

на заседании кафедры информационных техно-
логий и высшей математики

24 февраля 2025 г. протокол № 6

Заведующий кафедрой

Л.И. Трухина



**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(ФОНД ОЦЕНОЧНЫХ СРЕДСТВ)
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
Б1.У.10 Информационная безопасность**

Направление подготовки: 38.03.05 Бизнес-информатика

Направленность (профиль): Цифровая экономика

Квалификация выпускника: бакалавр

Чита, 2025 г.

**Структура
фонда оценочных средств
по дисциплине «Информационная безопасность»**

№ п/п	Этапы формирования компетенций	Перечень формируемых компетенций	ЗУНы (З.1, У1, Н1...)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы	Описание показателей и критериев оценивания компетенций на различных этапах формирования, описания шкал оценивания
1	Основные понятия информационной безопасности	ПК-2	З.Знать место и роль информационной безопасности в системе национальной безопасности Российской Федерации У.Уметь формулировать требования по обеспечению безопасности информации Н.Владеть методами формирования требований по защите информации	Уо, К	15-25 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 5-15 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применения навыков; 3-5 балла — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 2 и менее баллов — студент обнаружил несостоятельность ответов
2	Криптографические способы защиты информации	ПК-2	З.Знать типовые криптографические протоколы и стандарты У.Уметь пользоваться программными средствами,	Уо, Л	15-25 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно приме-

			<p>реализующими основные криптографические функции, такие, как системы публичных ключей, формирования цифровой подписи</p> <p>Н. Владеть способами защиты информации криптографическими методами и средствами</p>		<p>няемые навыки; 5-15 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применения навыков; 3-5 балла — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 2 и менее баллов — студент обнаружил несостоятельность ответов</p>
3	Антивирусная защита	ПК-2	<p>З. Знать механизмы реализации вредоносных программно-технических и информационных воздействий в инфокоммуникационных системах</p> <p>У. Уметь определять актуальные источники угроз безопасности для различных профессиональных областей</p> <p>Н. Владеть навыками работы с антивирусными программами (проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы)</p>	Уо, К	<p>15-25 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 5-15 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применения навыков; 3-5 балла — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 2 и</p>

					менее баллов — студент обнаружил несостоятельность ответов
4	Сетевая безопасность	ПК-2	<p>З.Знать технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации</p> <p>У.Уметь эксплуатировать инженерно-технические средства обеспечения информационной безопасности</p> <p>Н.Владеть навыками поддержки инженерно-технических средств обеспечения информационной безопасности защищенных информационно-коммуникационных систем</p>	Уо, К	<p>15-25 баллов — сформированные систематические знания; на высоком уровне осуществляемые умения, успешно применяемые навыки; 5-15 баллов — сформированные, но содержащие отдельные пробелы знания; в целом успешные, но содержащие отдельные пробелы умения; в целом успешное, но содержащее отдельные пробелы применение навыков; 3-5 балла — общие, но не структурированные знания; не систематически осуществляемые умения; не систематически применяемые навыки; 2 и менее баллов — студент обнаружил несостоятельность ответов</p>
5	Итого по текущей аттестации	ПК-2			100
6	Промежуточная аттестация	ПК-2			100

Министерство науки и высшего образования Российской Федерации
ЧИТИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)
ФГБОУ ВО «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кафедра информационных технологий и высшей математики

ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ

1. Свойства информации в форме сообщения:

- a. идеальность
- b. субъективность
- c. информационная неуничтожаемость
- d. динамичность
- e. материальность
- f. накапливаемость

2. Свойства информации в форме сведений: (укажите правильный вариант)

- a. материальность
- b. измеримость
- c. сложность
- d. проблемная ориентированность
- e. накапливаемость

3. Информационная сфера – это ... , ... , ... ,

4. Первая классификация национальных интересов:

- a. интересы ...
- b. интересы ...
- c. интересы ...

5. Общие методы обеспечения информационной безопасности:

- a. ...
- b. ...
- c. ...

6. Информация – наиболее ценный ... современного общества.

7. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?

- a. Документы
- b. Персонал
- c. Организационные единицы
- d. Промышленные образцы
- e. Научный инструментарий

8. Поставьте в порядке важности национальные интересы:

- a. Информационное обеспечение государственной политики Российской Федерации.
- b. Развитие современных информационных технологий, отечественной индустрии информации.
- c. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею.
- d. Защита информационных ресурсов от несанкционированного доступа

9. Допишите различные подходы к понятию информации:

- a. информация ...
- b. информация ...
- c. ... информация

10. Составляющие национальной безопасности:

- a. ...
- b. ...
- c. ...

ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.
2. Основные составляющие и аспекты информационной безопасности.
3. Классификация угроз информационной безопасности: для личности, для общества, для государства.
4. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.
5. Концепция «информационной войны» по оценкам российских спецслужб.
6. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?
7. Сфера применения информационного оружия.
8. Особенности информационного оружия. Организация защиты.
9. Основные задачи в сфере обеспечения информационной безопасности.
10. Отечественные стандарты в области информационной безопасности
11. Зарубежные стандарты в области информационной безопасности
12. Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?
13. Основные критерии оценки надёжности: политика безопасности и гарантированность.
14. Понятие государственной тайны. Понятие профессиональной тайны.
15. Понятие коммерческой тайны. Понятие служебной тайны. Понятие банковской тайны.
16. Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере.
17. Понятие надёжности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.
18. Уязвимость информации в автоматизированных системах обработки данных.
19. Элементы и объекты защиты в автоматизированных системах обработки данных.
20. Методы защиты информации от преднамеренного доступа.
21. Защита информации от исследования и копирования.
22. Опознавание с использованием простого пароля. Метод обратимого шифрования.
23. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
24. Использование динамически изменяющегося пароля. Метод «запрос-ответ»
25. Использование динамически изменяющегося пароля. Функциональные методы
26. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.
27. Электронная (цифровая) подпись. Цели применения электронной подписи.
28. Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.

29. Классификация методов криптографического закрытия.
30. Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.
31. Угрозы информации в персональных ЭВМ.
32. Обеспечение целостности информации в ПК. Физическая защита ПК и носителей информации.
33. Защита ПК от несанкционированного доступа.
34. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации. Дать краткую характеристику.
35. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки.
36. Программные закладки. Классификация критериев вредоносного воздействия закладок.
37. Общие характеристики закладок.
38. Методы и средства защиты от закладок.
39. Компьютерный вирус. Какая программа считается зараженной.
40. По каким признакам классифицируются вирусы?
41. Способы заражения программ. Стандартные методы заражения.
42. Как работает вирус?
43. Методы защиты от вирусов.
44. Антивирусные программы. Программы-детекторы. Программы-доктора.
45. Антивирусы-полифаги. Эвристические анализаторы.
46. Программы-ревизоры. Программы-фильтры.
47. Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.
48. В чём заключаются задачи защиты в сетях передачи данных?
49. Проблемы защиты информации в вычислительных сетях.
50. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.
51. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.
52. Архитектура механизмов защиты информации в сетях ЭВМ.

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УМЕНИЙ

1. Лабораторная работа №1. Формальные модели безопасности.
2. Лабораторная работа №2: Методика определения информационных рисков.
3. Лабораторная работа №3: Шифрование сообщений методом Вижинера.
4. Лабораторная работа №4: Блочное шифрование информации методом гаммирования.
5. Лабораторная работа №5: Электронная жеребьевка.
6. Лабораторная работа №6: Шифрование информации методом RSA.
7. Лабораторная работа №7: Электронная подпись.

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ

- Практическая работа 1. Анализ источников, каналов распространения и каналов утечки информации.
- Практическая работа 2. Проведение анализа информации на предмет целостности.
- Практическая работа 3. Оценка уязвимости информации.
- Практическая работа 4. Требования к безопасности информационных систем.
- Практическая работа 5. Требования к безопасности информационных систем в России.

Практическая работа 7. Определение классов защищенности средств вычислительной техники от несанкционированного доступа.

Практическая работа 8. Определение требований к защите информации.

Практическая работа 9. Анализ терминов и определений информационной безопасности.

Практическая работа 10. Работа с ГОСТами в области информационной безопасности.

Практическая работа 11. Составление инструкции по обработке и хранению конфиденциальных документов.

Практическая работа 12. Определение коэффициента важности, полноты, адекватности, релевантности, толерантности информации.

Практическая работа 13. Оценка безопасности информации на объектах ее обработки.

Практическая работа 14. Классификация автоматизированных систем обработки информации по классу защиты информации.

Практическая работа 15. Планирование, создание и изменение учетных записей пользователей.

Практическая работа 16. Создание и администрирование групп пользователей.

Практическая работа 17. Планирование и установка разрешений NTFS для файлов, папок отдельным пользователям и группам.

Практическая работа 18. Наследование разрешений в NTFS.

Практическая работа 19. Изменение параметров учетных записей пользователей.

Практическая работа 20. Настройка политики учетных записей.

Министерство науки и высшего образования
Российской Федерации
Читинский институт (филиал)
Федерального государственного бюджетного
образовательного учреждения высшего
образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-
информатика
Профиль - Цифровая экономика
Кафедра информационных техно-
логий и высшей математики
Дисциплина – Информационная без-
опасность

БИЛЕТ № 1

1. Типы объектов защиты информации и их определения.
2. Законодательные акты, регламентирующие работу со сведениями, составляющими государственную тайну.
3. Сферы применения симметричного и асимметричного шифрования.

Составитель _____ Е.А. Михайлова
Заведующий кафедрой _____ Л.И. Трухина

Министерство науки и высшего образования
Российской Федерации
Читинский институт (филиал)
Федерального государственного бюджетного
образовательного учреждения высшего
образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-
информатика
Профиль - Цифровая экономика
Кафедра информационных техно-
логий и высшей математики
Дисциплина – Информационная без-
опасность

БИЛЕТ № 2

1. Свойства информации, обеспечиваемые при её защите.
2. Законодательные акты, регламентирующие работу с персональными данными.
3. Примеры криптографических средств защиты информации.

Составитель _____ Е.А. Михайлова
Заведующий кафедрой _____ Л.И. Трухина

Министерство науки и высшего образования
Российской Федерации
Читинский институт (филиал)
Федерального государственного бюджетного
образовательного учреждения высшего
образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-
информатика
Профиль - Цифровая экономика
Кафедра информационных техно-
логий и высшей математики
Дисциплина – Информационная без-
опасность

БИЛЕТ № 3

1. Категории доступа к информации. Степени секретности сведений, составляющих государственную тайну.
2. Законодательные акты, регламентирующие работу со сведениями, составляющими служебную и коммерческую тайну.
3. Виды лицензируемой деятельности по криптографической защите информации.

Составитель _____ Е.А. Михайлова
Заведующий кафедрой _____ Л.И. Трухина

Министерство науки и высшего образования
Российской Федерации
Читинский институт (филиал)
Федерального государственного бюджетного
образовательного учреждения высшего
образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-
информатика
Профиль - Цифровая экономика
Кафедра информационных техно-
логий и высшей математики
Дисциплина – Информационная без-
опасность

БИЛЕТ № 4

1. Виды информации, относящейся к сведениям конфиденциального характера.
2. Основные функции ФСБ России в области обеспечения информационной безопасности.
3. Требования по сертификации криптографических средств защиты информации.

Составитель _____ Е.А. Михайлова
Заведующий кафедрой _____ Л.И. Трухина

Министерство науки и высшего образования
Российской Федерации
Читинский институт (филиал)
Федерального государственного бюджетного
образовательного учреждения высшего
образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-
информатика
Профиль - Цифровая экономика
Кафедра информационных техно-
логий и высшей математики
Дисциплина – Информационная без-
опасность

БИЛЕТ № 5

1. Понятие «нарушение информационной безопасности». Примеры атак на информационные системы.
2. Основные функции ФСТЭК России в области обеспечения информационной безопасности.
3. Нормативные документы ФСБ России по защите персональных данных.

Составитель _____ Е.А. Михайлова
Заведующий кафедрой _____ Л.И. Трухина

Министерство науки и высшего образования
Российской Федерации
Читинский институт (филиал)
Федерального государственного бюджетного
образовательного учреждения высшего
образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-
информатика
Профиль - Цифровая экономика
Кафедра информационных техно-
логий и высшей математики
Дисциплина – Информационная без-
опасность

БИЛЕТ № 6

1. Понятие «угроза информационной безопасности». Формы представления информации.
2. Правовые документы, устанавливающие ответственность за компьютерные преступления.
3. Примеры средств программно-аппаратной защиты информации.

Составитель _____ Е.А. Михайлова
Заведующий кафедрой _____ Л.И. Трухина

Министерство науки и высшего образования
Российской Федерации
Читинский институт (филиал)
Федерального государственного бюджетного
образовательного учреждения высшего
образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-
информатика
Профиль - Цифровая экономика
Кафедра информационных техно-
логий и высшей математики
Дисциплина – Информационная без-
опасность

БИЛЕТ № 7

1. Угрозы конфиденциальности информации, представленной в различных формах.
2. Правовые документы, устанавливающие ответственность за разглашение персональных данных.
3. Права на результаты интеллектуальной деятельности и средства индивидуализации.

Составитель _____ Е.А. Михайлова
Заведующий кафедрой _____ Л.И. Трухина

Министерство науки и высшего образования
Российской Федерации
Читинский институт (филиал)
Федерального государственного бюджетного
образовательного учреждения высшего
образования
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ»
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-
информатика
Профиль - Цифровая экономика
Кафедра информационных техно-
логий и высшей математики
Дисциплина – Информационная без-
опасность

БИЛЕТ № 8

1. Угрозы целостности информации, представленной в различных формах.
2. Правовые документы, устанавливающие ответственность за разглашение персональных данных.
3. Виды сертификатов соответствия средств защиты информации.

Составитель _____ Е.А. Михайлова
Заведующий кафедрой _____ Л.И. Трухина

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Система критериев оценки определяет оценку успеваемости по каждому заданию (вопросу) экзаменационного билета или заданию для зачета с использованием интервальной шкалы баллов, применяемой в привязке к рейтинговой 100-балльной системе.

ОЦЕНКА ОТВЕТА НА ТЕОРЕТИЧЕСКИЙ ВОПРОС В УСТНОЙ ИЛИ ПИСЬМЕННОЙ ФОРМЕ:

Оценка «отлично» / «зачтено» (91-100 баллов) выставляется при соблюдении следующих условий: Ответ отличается глубиной и полнотой, свободным владением понятийно-категориальным (терминологическим) аппаратом изученной дисциплины. Отражает знание не только основной, но и дополнительной литературы. Приведены примеры, отражающие умение связать теорию с практикой. Ответ изложен логически последовательно, грамотно и корректно.

Оценка «хорошо» / «зачтено» (76-90 баллов) выставляется при соблюдении следующих условий: Ответ отличается полнотой, владением понятийно-категориальным (терминологическим) аппаратом изученной дисциплины, но в ответе могут присутствовать неточности. Отражает знание основной литературы. Приведены примеры, отражающие умение связать теорию с практикой. Ответ изложен логически последовательно, грамотно и корректно, но недостаточно аргументирован.

Оценка «удовлетворительно» / «зачтено» (61-75 баллов) выставляется при соблюдении следующих условий: в ответе отражено знание понятийно-категориального (терминологического) аппарата изучаемой дисциплины, но присутствуют отдельные ошибки и неточности. Ответ характеризуется недостаточным знанием рекомендованной литературы. Примеры, отражающие умение связать теорию с практикой, тривиальны, либо отсутствуют. Ответ неполный, носит фрагментарный, непоследовательный характер.

Оценка «неудовлетворительно» / «не зачтено» (0-60 баллов) выставляется при соблюдении следующих условий: Ответ характеризуется незнанием, либо фрагментарным представлением о понятийно-категориальном аппарате дисциплины, содержит множество ошибок. Примеры и иллюстрации отсутствуют. Ответ логически непоследователен.

ОЦЕНКА ВЫПОЛНЕНИЯ ЗАДАНИЯ В ФОРМЕ CASE-STUDY (СИТУАЦИИ)

Оценка «отлично» / «зачтено» (91-100 баллов) выставляется при соблюдении следующих условий: Четкая формулировка проблемы. Полное и соответствующее ситуации решение, основанное на знании правовых норм и технологий (опыте), применяемых в реальных организациях (известных компаниях). Предполагаемые действия описаны логично и последовательно. Даны дополнительные авторские комментарии и предложения к решению ситуации.

Оценка «хорошо» / «зачтено» (76-90 баллов) выставляется при соблюдении следующих условий: Понимание сути проблемы, но ее формулирование затруднено. Решение соответствует ситуации, отражает знание правовых норм и опыт работы других организаций при решении подобных ситуаций. Логика и последовательность действий не нарушены.

Оценка «удовлетворительно» / «зачтено» (61-75 баллов) выставляется при соблюдении следующих условий: Проблема не сформулирована. Приведен набор действий, потенциально способствующих улучшению ситуации и решению проблемы.

Оценка «неудовлетворительно» / «не зачтено» (0-60 баллов) выставляется при соблюдении следующих условий: Предложенный перечень мероприятий не соответствует

ситуации.

ОЦЕНКА РЕШЕНИЯ ЗАДАЧИ

Оценка «отлично» / «зачтено» (91-100 баллов) выставляется при соблюдении следующих условий: Полное верное решение - оценивается в n баллов (n – максимальное количество баллов за решение задачи в структуре экзаменационного билета/задания).

Оценка «хорошо» / «зачтено» (76-90 баллов) выставляется при соблюдении следующих условий: Верное решение; имеются небольшие недочеты, в целом не влияющие на решение – оценивается в диапазоне от $0,76 \cdot n$ баллов до $0,9 \cdot n$ баллов (n – максимальное количество баллов за решение задачи в структуре экзаменационного билета/задания).

Оценка «удовлетворительно» / «зачтено» (61-75 баллов) выставляется при соблюдении следующих условий: Решение в целом верное; однако оно содержит ряд ошибок, либо не учитывает отдельных случаев, но может стать правильным после некоторых исправлений или дополнений – оценивается в диапазоне от $0,61 \cdot n$ баллов до $0,75 \cdot n$ баллов (n – максимальное количество баллов за решение задачи в структуре экзаменационного билета/задания).

Оценка «неудовлетворительно» / «не зачтено» (0-60 баллов) выставляется при соблюдении следующих условий: Решение неверное; изначально выбран неверный ход решения, или решение отсутствует – оценивается в 0 баллов.

ОЦЕНКА ВЫПОЛНЕНИЯ ТЕСТОВОГО ЗАДАНИЯ

Подсчитывается доля набранных баллов в максимальной сумме баллов за все задания теста:

- каждый правильный ответ на тестовый вопрос (тип выборочный, одинарный, множественный, открытый) оценивается в m баллов (число m определяется путем деления максимального количества баллов за выполнение теста в структуре экзаменационного билета/задания на количество тестовых заданий);

- каждый частично правильный ответ на тестовый вопрос (тип выборочный, множественный, открытый) оценивается в $m/2$ баллов независимо от соотношения правильно/неправильно выбранных вариантов (число m определяется путем деления максимального количества баллов за выполнение теста в структуре экзаменационного билета/задания на количество тестовых заданий);

- каждый неправильный ответ на тестовый вопрос (тип выборочный, одинарный) оценивается в 0 баллов.

Оценка «отлично»/«зачтено» (91-100 баллов) выставляется, если доля набранных баллов составляет 91-100%.

Оценка «хорошо»/«зачтено» (76-90 баллов), если доля набранных баллов составляет 76-90%.

Оценка «удовлетворительно»/«зачтено» (61-75 баллов), если доля набранных баллов составляет 61-75%.

Оценка «неудовлетворительно»/«не зачтено» (0-60 баллов), если доля набранных баллов составляет не более 60%.