Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автономных информационных и управляющих систем

Паспорт зачета

по дисциплине «Организационное и правовое обеспечение информационной безопасности», 2 семестр

1. Методика оценки

Зачет проводится в письменной форме по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-34, второй вопрос из диапазона вопросов 35-56 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФЛА

Билет № _____
к зачету по дисциплине «Организационное и правовое обеспечение информационной безопасности»

---

1. Вопрос 1
2. Вопрос 2.

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

Пример билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФЛА

Билет № 7
к зачету по дисциплине «Организационное и правовое обеспечение информационной безопасности»

Вопрос 1) Национальной безопасность Российской Федерации

Вопрос 2) Анализ и оценка угроз информационной безопасности объекта

Утверждаю: зав. кафедрой АИУС _____ Легкий В.Н.
(подпись)
(дата)

2. Критерии оценки

- Ответ на билет для зачета считается неудовлетворительным, если даны неверные ответы на вопросы, или ответы отсутствуют, оценка составляет 0-4 баллов.
- Ответ на билет (тест) для зачета засчитывается на **пороговом** уровне, если даны неточные ответы на вопросы, оценка составляет 5 баллов за вопрос и 10 баллов за работу.
- Ответ на билет (тест) для зачета билет засчитывается на **базовом** уровне, если даны неполные ответы на вопросы, оценка составляет 6 - 9 баллов за вопрос и 12-18 баллов за работу в зависимости от полноты ответов.
- Ответ на билет (тест) для зачета билет засчитывается на **продвинутом** уровне, если даны правильные и полные ответы на вопросы, оценка составляет 10 баллов за вопрос и 20 баллов за работу.

3. Шкала оценки

Оценка знаний и умений студентов проводится с помощью вопросов по основным проблемам дисциплины. Для оценки деятельности студента используются зачетные задания в виде **2-х теоретических вопросов.** Теоретические вопросы формулируются в строгом соответствии с темами лекционных занятий. Максимальное количество баллов, которое студент может получить на зачете, равно **20.**

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 10 баллов (из 20 возможных). Устанавливаются следующие правила аттестации студента (таблица 1).

Таблица 1

Характер ответа	**Количество баллов за ответ**
Правильный ответ на вопрос	10
Неполный ответ на вопрос	6 - 9
Неточный ответ на вопрос	5

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** зачету **по дисциплине «**Организационное и правовое обеспечение информационной безопасности**»**

1. Информационная безопасность
2. Аспекты информационной безопасности
3. Уровни формирования режима информационной безопасности
4. Основные задачи в сфере обеспечения информационной безопасности, определяемым государством
5. Информационная сфера
6. Информационное законодательство
7. Законодательство в информационной сфере
8. Законодательство в области обеспечения информационной безопасности
9. Концепция национальной безопасности Российской Федерации
10. Национальной безопасность Российской Федерации
11. Национальные интересы России
12. Доктрина информационной безопасности Российской Федерации
13. Основные составляющие национальных интересов Российской Федерации в информационной сфере
14. Основные объекты информационной безопасности государства
15. Собственник защищаемой информации
16. Владелец защищаемой информации
17. Три группы информационных ресурсов государства
18. Отличительные признаки защищаемой информации
19. Классификация информации по степени ее секретности
20. Владельцы (собственники) защищаемой информации
21. Носители информации
22. Классификация носителей защищаемой информации
23. Документ Изделия (предметы) как носители защищаемой информации
24. Определение понятия «Государственная тайна»
25. Какие сведения следует относить
    - к сведениям особой важности
    - к совершенно секретным сведениям
    - к секретным сведениям
26. Какую информацию нельзя засекречивать
27. Политический ущерб
28. Экономический ущерб
29. Моральный ущерб
30. Определение понятия «Коммерческая тайна»
31. Какая информация составляет коммерческую тайну предприятия
32. Объекты интеллектуальной собственности
33. Сведения, которые не могут составлять коммерческую тайну
34. Степени секретности коммерческой тайны (перечислить)
35. Требования обеспечения безопасности
36. Задачи, которые решает комплексная защита КИ
37. Работа с персоналом
38. Политика безопасности и процедуры внутрифирменной коммуникации
39. Сервисы безопасности
40. Правовые аспекты применения технических средств получения и защиты информации

41. Принципы инженерно-технической защиты информации
42. Пассивные и активные способы защиты информации
43. Организационная защита
44. Технические мероприятия
45. Основные методы защиты информации техническими средствами
46. Защита интеллектуальной собственности
47. Объект авторского права.
48. Товарный знак
49. Анализ и оценка угроз информационной безопасности объекта
50. Анализ информационных рисков
51. Аудит информационной безопасности
52. Работы по аудиту безопасности ИС
53. Система физической защиты, комплексная система безопасности
54. Процесс создания (модернизации) СФЗ, КСБ. Концептуальное проектирование СФЗ.
55. Пути построения и модернизации СФЗ. Проблемы построения СФЗ
56. Оценка эффективности СФЗ