Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра вычислительной техники
Кафедра защиты информации

Паспорт зачета

по дисциплине «Криптографические методы защиты информации», 2семестр

1. Методика оценки

Зачет проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-6, второй вопрос из диапазона вопросов 7-12 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Криптографические методы защиты информации»

---

1. Длина ключа и стойкость шифра.
2. Отечественные стандарт хэш-функции ГОСТ Р 34.11-2012.

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

2. **Критерии оценки**

- Ответ на зачетный билет считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *_5_ баллов.*
- Ответ на зачетный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные,
  оценка составляет *10 баллов.*
- Ответ на зачетный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов,

явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет *_15_ баллов.*

- Ответ на зачетный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет _20_ *баллов.*

3. Шкала оценки

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

4. **Вопросы к** зачету **по дисциплине** «Криптографические методы защиты информации»

1	Криптографическая защита информации. Классификация шифров. Требования к средствам криптографической защиты информации.
2	Шифры и шифрование. Основные понятия и определения
3	Шифры перестановки
4	Шифры замены
5	Шифр гаммирования
6	Шифр гаммирования с обратной связью
7	Совершенные, идеально стойкие, абсолютно стойкие шифры
8	Длина ключа и стойкость шифра
9	Фундаментальные ограничения криптографических преобразований
10	Проблемы массового использования шифров. Стандартные схемы и приемы реализации массовых шифров.
11	Стандартные шифры (DES, ГОСТ, AES).
12	Стандарт шифрования DES.
13	Режимы использования шифра DES
14	Стандарт шифрования ГОСТ 28147-89
15	Стандарт шифрования AES
16	Генераторы псевдослучайных чисел в шифровании
17	Основные подходы и методики криптоанализа.
18	Криптоанализ с использованием открытого текста.
19	Криптосистемы с открытым ключем. Принцип Шеннона. Основные особенности и характеристики криптосистем с открытым ключем
29	Структура системы секретной связи при использовании симметричных шифров и шифров с открытым ключом
21	Система Диффи-Хелмана
22	Шифр RSA
23	Шифр Эль Гаммаля
24	Гибридные криптосистемы
25	Основные проблемы криптографической защиты и способы их решения

26	Применение шифров для идентификации и аутентификации субъектов и данных. Хэш-функции. Электронно-цифровая подпись. Схемы цифровой подписи.
27	Отечественные стандарт хэш-функции ГОСТ Р 34.11-2012
28	Отечественные стандарт шифрования с открытым ключом и электронно-цифровой подписи ГОСТ Р 34.10-2012