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

Паспорт экзамена

по дисциплине «Методы и средства криптографической защиты информации», 5 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. Билет состоит из 2 вопросов и формируется по следующему правилу:

- первый вопрос выбирается из диапазона вопросов 1-12;
- второй вопрос из диапазона вопросов 13-25.

Таким образом, проверяются результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

На экзамене преподаватель вправе задавать студенту уточняющие и дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к экзамену по дисциплине «Методы и средства криптографической защиты информации»

---

1. Вопрос 1
2. Вопрос 2.

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

2. Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент проводит сравнительный комплексный анализ материала, выявляет проблемы, предлагает механизмы их решения, представляет количественные характеристики определенных процессов, приводит конкретные примеры. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций не

содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от 35 до 40 баллов.*

Ответ на экзаменационный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, дает характеристику процессов, явлений, проводит анализ причин, условий, способен представить количественные и качественные характеристики процессов. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от 34 до* 27 *баллов.*

Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от* 26 *до* 20 *баллов.*

Ответ на экзаменационный билет считается **неудовлетворительным** (ниже порогового уровня), если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений. Совокупность результатов обучения по дисциплине и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее* 20 *баллов.*

3. Шкала оценки

Экзамен считается сданным, если сумма баллов по всем заданиям билета составляет от 20 до 40 баллов включительно. Сумма менее 20 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине.

В общей оценке по дисциплине экзаменационные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Вопросы к экзамену по дисциплине «Методы и средства криптографической защиты информации»

1. Предмет криптографии – основные понятия и определения, направления и приложения криптографии.
2. Симметричные и несимметричные криптосистемы. Схемы ЭЦП.
3. Классификация шифров. Исторические шифры. Шифры замены. Примеры.
4. Классификация шифров. Исторические шифры. Шифры перестановки. Примеры.
5. Классификация шифров. Исторические шифры. Шифры гаммирования. Пример.
6. Шифровальные машины ENIGMA и Hagelin (M-209).
7. Атаки и угрозы криптосистеме. Понятие стойкости. Вычислительная стойкость, теоретическая стойкость.
8. Математическая модель шифра (алгебраическая и вероятностная модели).
9. Блочные шифры – основные принципы.
10. Алгоритм шифрования DES – параметры шифра, основные шаги шифрования.
11. Шифр ГОСТ 28147-89 – параметры, основные шаги шифрования.
12. Основы проектирования блочных шифров. Рассеивание и перемешивание.
13. Сочетание блочных шифров.
14. Режимы блочных шифров.
15. Энтропийные характеристики шифрсистем.
16. Теория секретности Шеннона. Идеальные шифры. Совершенные шифры.
17. Кольца и поля многочленов. Операции в Z2[x].

18. Шифр SQUARE.
19. Операции шифрования и расшифрования в шифре Rijndael (AES).
20. Формирование раундовых ключей в шифре Rijndael (AES).
21. Чистые шифры.
22. Шифры, не распространяющие замен символов.
23. Шифры, не распространяющие выпадений – вставок символов.
24. Защитные контрольные суммы – основные понятия и определения. Понятие хэш-функции. Требования к хэш-функциям. Понятие коллизии. Криптографическая стойкость хэш-
функций.
25. Общая схема построения бесключевой хэш-функции.