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

Паспорт
расчетно-графического задания (работы)

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

1. Методика оценки

Выполнение расчетно-графического задания (работы) (далее - РГЗ(Р)) является формой текущей аттестации (контроля) по дисциплине, предусмотренной учебным планом.

Цель РГЗ(Р): студенты должны освоить и научиться программной реализации принципов, методов и алгоритмов решения криптографических задач.

Обязательным элементом РГЗ(Р) является решение криптографических задач.

Номер задания соответствует последней цифре (цифрам) в номере зачетной книжки (студенческого билета).

РГЗ(Р) выполняется индивидуально.

Количество заданий достаточно для обеспечения, каждого обучающегося индивидуальным заданием РГЗ(Р).

Замена задания РГЗ(Р) осуществляется по согласованию с преподавателем из числа резервных (не занятых) заданий.

Преподаватель осуществляет руководство по выполнению задания, оказывает консультационную помощь и принимает отчет по РГЗ(Р).

По результатам выполнения РГЗ(Р) выполняется отчет, который состоит из следующих частей:

1. титульный лист;
2. введение;
3. теоретическая часть;
4. практическая часть;
5. заключение;
6. список литературы;
7. приложения (при необходимости).

Требования к оформлению:

Объем РГЗ(З) до 50 страниц машинописного текста формата А4. Шрифт Times New Roman, 12. Формулы набираются в редакторе Math Type. Размещение сканированных формул не допускается. Нумерация страниц сквозная, в нижней части листа по центру арабскими цифрами. Работа должна быть отредактирована, не содержать орфографических, синтаксических и стилевых ошибок.

Отчет в установленные сроки сдается на кафедру для проверки. Преподаватель оценивает качество работы, отмечает положительные стороны и недостатки работы и определяет, допускается ли она к защите. При необходимости преподаватель возвращает РГЗ(Р) студенту для доработки и устанавливает сроки повторного предоставления для проверки. До защиты работы студентом должны быть сделаны необходимые исправления и дополнения по всем замечаниям преподавателя.

При положительном результате оценивания РГЗ(Р) студент её распечатывает, передает на кафедру и защищает до сессии в назначенное преподавателем время.

Защита РГЗ(Р) состоит в индивидуальном устном собеседовании студента с преподавателем. В процессе защиты выявляется уровень знаний студента, степень его самостоятельности при выполнении работы. По результатам защиты студенту выставляется оценка в соответствии с критериями, приведенными в п. 2 настоящего Паспорта.

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

Общие правила выставления оценок текущей аттестации определяются балльно-рейтинговой системой, установленной локальным актом НГТУ.

РГЗ(Р) считается выполненной **на продвинутом** уровне, если все необходимые расчеты произведены самостоятельно и без ошибок; все разделы РГЗ(Р) выполнены правильно и в полном объеме; работа оформлена в соответствии с требованиями; сдана преподавателю в указанные сроки и не возвращалась для доработки; даны полные и развернутые выводы и рекомендации; на защите студентом даны уверенные и аргументированные ответы. Совокупность запланированных результатов и соотнесенных с ними индикаторов достижения компетенций не содержит пробелов. Закрепленные за РГЗ(Р) компетенции сформированы на продвинутом уровне. Оценка составляет *от 26 до 30 баллов.*

РГЗ(Р) считается выполненной **на базовом** уровне, если все необходимые расчеты произведены самостоятельно и без существенных ошибок; все разделы РГЗ(Р) выполнены правильно, но есть замечания к полноте предоставления информации; работа оформлена в соответствии с требованиями; сдана преподавателю в указанные сроки и однократно возвращалась студенту для незначительной доработки; в заключении даны выводы и рекомендации; на защите студентом допущены непринципиальные ошибки. Совокупность запланированных результатов и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Закрепленные за РГЗ(Р) компетенции сформированы на базовом уровне. Оценка составляет *от 21 до 25 баллов.*

РГЗ(Р) считается выполненной **на пороговом** уровне, если все необходимые расчеты произведены самостоятельно, но с ошибками, часть из которых носит принципиальный характер; есть замечания к полноте предоставления информации; работа оформлена в соответствии с требованиями; сдана преподавателю, но неоднократно возвращалась студенту для доработки; в заключении даны краткие выводы; защита РГЗ(Р) вызывает у студента серьезные затруднения. Совокупность запланированных результатов и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Закрепленные за РГЗ(Р) компетенции сформированы на пороговом уровне. Оценка составляет *от 15 до 20 баллов.*

РГЗ(Р) считается **не выполненной** (ниже порогового уровня), если расчеты произведены с серьезными ошибками; есть замечания к полноте предоставления информации и оформлению; РГЗ(Р) была сдана преподавателю, но неоднократно возвращалась студенту для доработки, что не привело к улучшению ее качества; РГЗ(Р) не допущена до защиты, что свидетельствует о неудовлетворительном уровне достигнутых студентом результатов. Совокупность запланированных результатов и соотнесенных с ними индикаторов достижения компетенций содержит множественные существенные пробелы. Закрепленные за РГЗ(Р) компетенции не сформированы. Оценка составляет менее 15 баллов.

3. Шкала оценки

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

РГЗ(Р) как форма текущей аттестации (контроля) по дисциплине считается успешно выполненной, если сумма полученных баллов по всем его заданиям составляет от 15 до 30 баллов включительно.

4. Примерный перечень тем РГЗ(Р)

1. Шифр одиночной перестановка по ключу.
2. Шифр двойной перестановка по ключу.
3. Шифр перестановки с запретом записи.
4. Шифр перестановки на основе «магического» квадрата.
5. Шифр перестановки «по маршрутам».
6. Шифр перестановки с различными размерами блоков.
7. Шифр простой перестановки с изменением направления записи/чтения.
8. Шифры замены. Система Цезаря.
9. Шифры замены. Система Полибия.
10. Шифры замены. Простая замена.
11. Шифр Гронсфельда.
12. Шифр Виженера.
13. Шифр многоалфавитной замены.
14. Шифр монофонической замены.
15. Шифр гаммирования.
16. Операции шифрования и расшифрования в шифре Rijndael(AES).
17. Формирование раундовых ключей в шифре Rijndael(AES).
18. Чистые шифры.
19. Шифры, не распространяющие замен символов.
20. Шифры, не распространяющие выпадений – вставок символов.
21. Защитные контрольные суммы.
22. Криптографическая стойкость хэш-функций.
23. Построение бесключевой хэш-функции.
24. Крипто протокол Диффи-Хеллмана.
25. Крипто протокол Эль-Гамаля.