МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

«Статический и формальный анализ исходных текстов криптографических программ»

Липницкий Станислав Юрьевич

Научный руководитель – кандидат физ.-мат. наук Агиевич С.В.

2017

АННОТАЦИЯ

Дипломная работа, 41 с., 5 источников.

ФОРМАЛЬНЫЕ МЕТОДЫ, СТАТИЧЕСКИЙ АНАЛИЗ, PVS-STUDIO, FRAMA-C.

Объект исследования – статический и формальный анализ исходных текстов.

Цель работы – ознакомиться и применить средства статического анализа и формальных методов к криптографической библиотеке bee2.

За время работы были решены следующие задачи:

– изучены концепции и средства статического анализа и формальных методов;

– проведён сравнительный анализ инструментов;

– изученные средства применены на практике к криптографической библиотеке bee2.

Методами исследования данной дипломной работы являются методы научно-практического исследования. Областью применения является анализ исходных текстов в криптографии.

ABSTRACT

Diploma thesis, 41 p., 5 sources.

FORMAL METHODS, STATIC ANALYSIS, PVS-STUDIO, FRAMA-C.

Object of research – Static and formal analysis of source code.

Purpose of research – To familiarize and apply means of static analysis and formal methods to the cryptographic library bee2.

During the work following tasks were solved:

- concepts and tools of static analysis and formal methods are studied;
- comparative analysis of tools;
- studied tools are applied in practice to the cryptographic library bee2.

Methods of research are practice-research. The field of application is analysis of source code in cryptography.