

Аннотация
к дипломной работе студента МФТИ (ГУ),
919 группы ФРТК, Перова М.Н. на тему
«Разработка кроссплатформенного динамического анализатора
бинарного кода на основе QEMU»

Тема дипломной работы – «Разработка кроссплатформенного динамического анализатора бинарного кода на основе QEMU».

Цель работы – создание инструмента динамического анализа бинарного кода, поддерживающего множество архитектур, встраивание новой архитектуры в который будет происходить в полуавтоматизированном режиме.

В данной работе:

1. Исследованы существующие инструменты, основанные на технологии DBI.
2. Реализован инструмент идентификации переполнения буфера в стеке в бинарном исполняемом файле.
3. Разработана технология автоматизации процесса встраивания новой архитектуры в QEMU.