Рецензия
на выпускную квалификационную работу
студента 444 группы математико-механического факультета СПбГУ
Небогатикова Ивана Юрьевича
«Мониторинг работы операционной системы в реальном времени на основе гипервизора»

В работе рассматривается гипервизорный подход к защите разрабатываемой Хановым Артуром Рафаэльевичем системы КОДА для поиска аномалий в поведении программ. Такой метод является эффективным решением, если надо взаимодействовать с Kernel Patch Protection, поскольку ее поведение не документировано.

В работе представлен подробный анализ предметной области, рассмотрены разные подходы защиты с использованием гипервизора.

Далее приводится обзор используемых инструментов, обосновывается их выбор.

В главе с реализацией описывается общая архитектура решения, то, как происходит взаимодействие с КОДОЙ. Также приведены детали реализации как гипервизорной части, так и защиты на основе драйверов. Проведены тесты производительности, подробно описаны условия тестирования и результаты.

В качестве недочетов работы можно выделить недостаточно подробное описание самой КОДЫ.

Цели, поставленные в работе выполнены. Выпускная квалификационная работа соответствует основным требованиям, предъявляемым к выпускной квалификационной работе бакалавра, и заслуживает оценки «отлично».

Воробьева Алиса Андреевна,
к.т.н., доцент факультета безопасности информационных технологий Университета ИТМО

Дата: Подпись:_____