Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «**Информатика и системы управления**»

КАФЕДРА «**Программное обеспечение ЭВМ и информационные технологии**»

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К НАЧУНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

НА ТЕМУ:

Анализ существующих реализаций доверенных сред исполнения (TEE)

Студент группы **ИУ7-32М** _____ **А. В. Романов**
(Подпись, дата) (И.О. Фамилия)

Руководитель НИР _____ **Д. Е. Бекасов**
(Подпись, дата) (И.О. Фамилия)

***2023** г.*

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Необходимость повышения безопасности исполнения приложений, работающих в системах безопасности и обрабатывающих защищаемую информацию, привела к разработке программно-аппаратных решений, создающих доверенные среды исполнения (англ. TEE – Trusted Execution Environment [1]) на базе аппаратных средств, доверенных загрузок или аппаратно-программных модулей доверенной загрузки. Intel [2] и ARM [3] являются лидерами в этой области. Целью данной работы является анализ и сравнение существующих реализаций доверенных сред исполнения (ДСИ).

Для достижения поставленной цели необходимо решить следующие задачи:

- провести обзор существующих реализаций ДСИ;
- описать плюсы и недостатки каждой из реализаций;
- сформулировать критерии сравнения;
- сравнить существующие реализации.

1 Анализ предметной области

В этом разделе будут проведен анализ предметной области:

2 Существующие реализации ДСИ

2.1 SGX Software Guard Extensions

Intel

2.2 Platform Security Processor

AMD

2.3 TrustZone

ARM

2.4 MultiZone TEE

Risc-V

3 Сравнение реализаций ДСИ

3.1 Критерии сравнения

ЗАКЛЮЧЕНИЕ

В ходе выполнения научно исследовательский работы была достигнута ее цель – проведен анализ и сравнение существующих реализаций ДСИ.

Для достижения данной цели были решены следующие задачи:

- проведён обзор существующих реализаций ДСИ;
- описаны плюсы и недостатки каждой из реализаций;
- сформулированы критерии сравнения;
- проведено сравнение существующих реализации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Introduction to Trusted Execution Environments – Global Platform [Электронный ресурс]. – Режим доступа: https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Trusted-Execution-Environment-15May2018.pdf, свободный – (09.10.2023)

2. Intel | Data Center Solutions, IoT, and PC Innovation [Электронный ресурс]. – Режим доступа: https://www.intel.com/, свободный – (10.11.2022)

3. Building the Future of Computing – Arm® [Электронный ресурс]. – Режим доступа: https://www.arm.com, свободный – (09.10.2022)