Метод программной реализации доверенной среды исполнения с помощью виртуализации процессоров архитектуры ARM

Квалификационная работа магистра

Студент группы ИУ7-42М: Романов Алексей Васильевич
Научный руководитель: Бекасов Денис Евгеньевич

Цель и задачи работы

Цель работы: разработка метода программной реализации доверенной среды исполнения с помощью виртуализации процессоров архитектуры ARM.

Задачи:

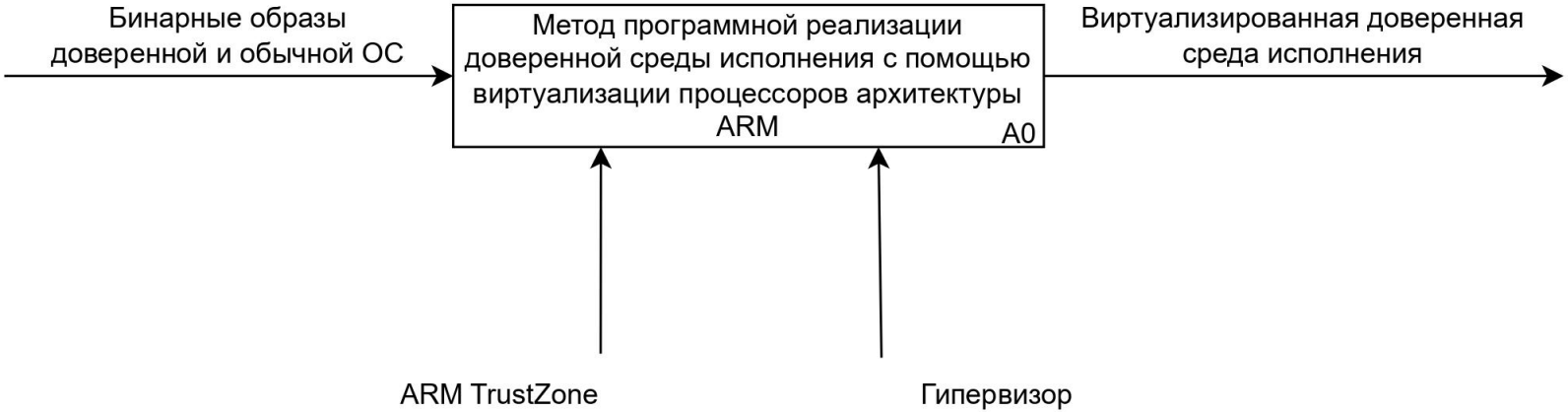
- провести анализ существующих реализаций доверенных сред исполнения
- спроектировать метод для платформ с архитектурой ARM
- спроектировать, реализовать и протестировать программные модули реализующие метод
- провести сравнение скорости работы разработанного программного обеспечения с аппаратной реализацией.

Сравнение реализаций доверенных сред исполнения

Доверенная среда исполнения	Производитель-ность	Проприетарное решение	Аппаратное решение	Поддержка виртуализации
ARM TrustZone	Средняя	Да	Да	Нет
Intel SGX	Высокая	Да	Да	Да
Keystone (RISC-V)	Низкая	Нет	Нет	-

ARM TrustZone – аппаратно реализованная доверенная среда исполнения не поддерживающая виртуализацию.

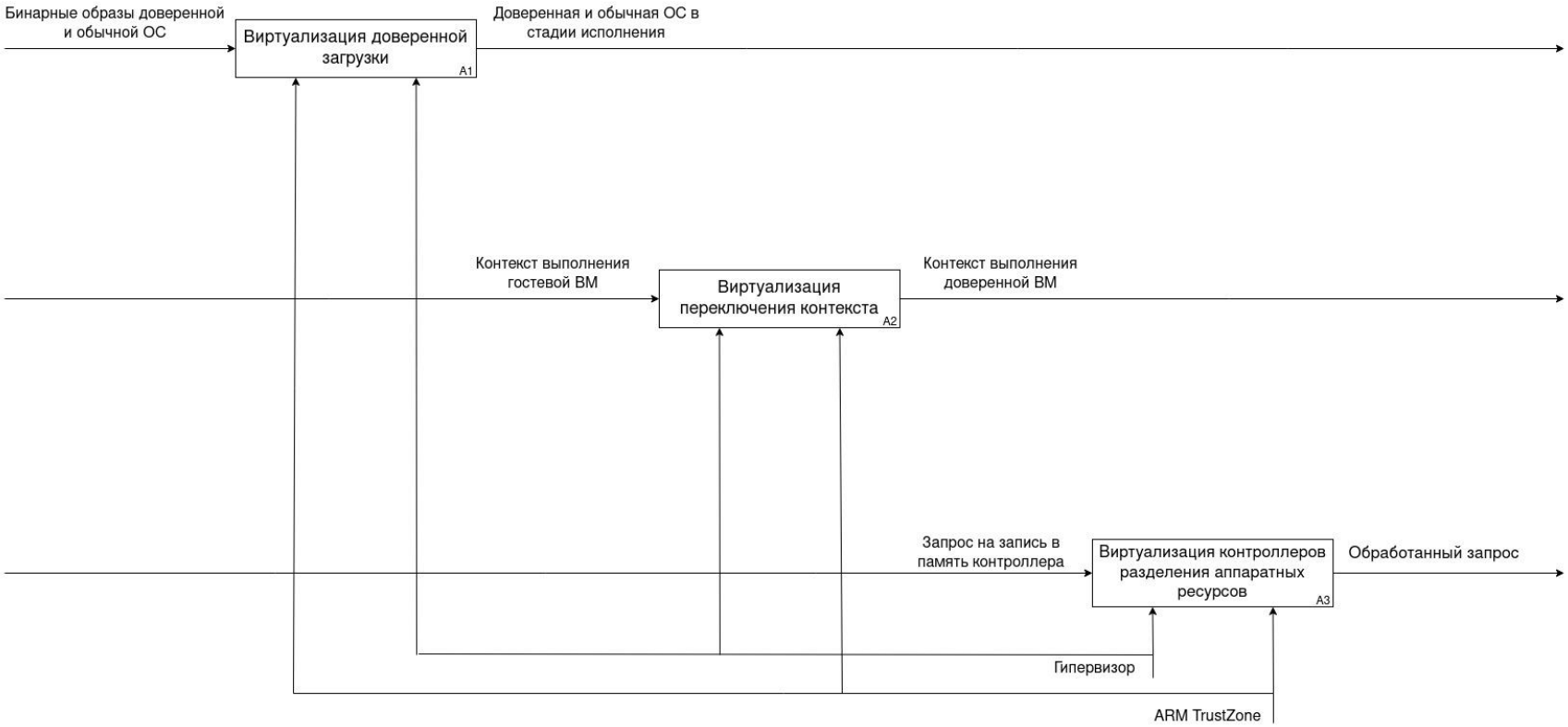
Постановка задачи



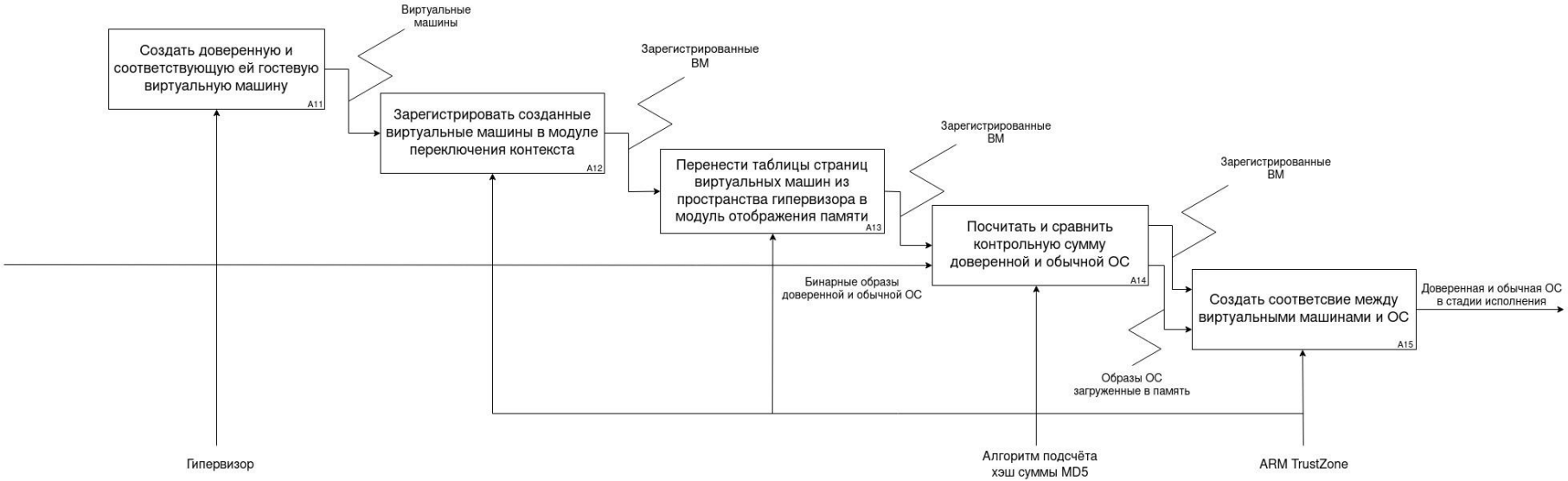
Дополнительные условия:

- Архитектура ARMv8 и новее
- Использовать механизмы аппаратной виртуализации ARM
- Должны поддерживаться все свойства безопасности предоставляемые аппаратной технологий ARM TrustZone

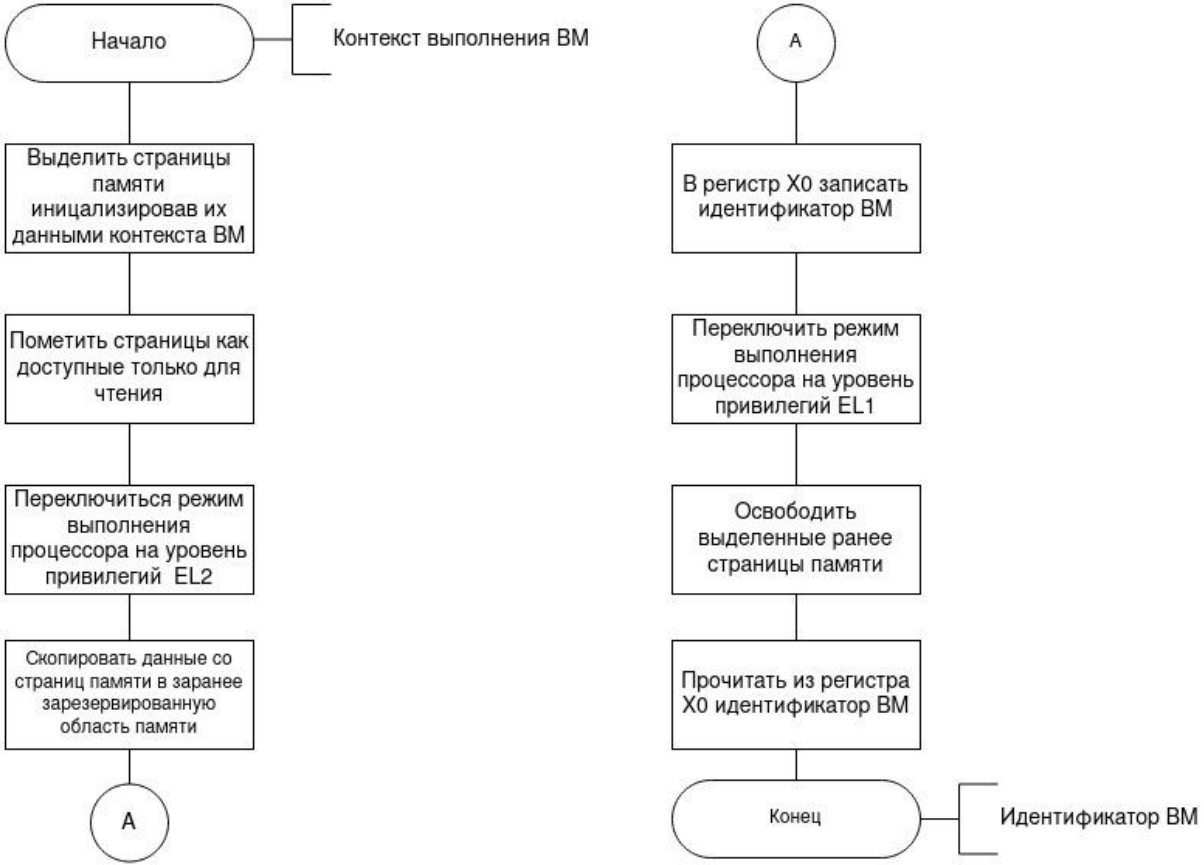
Детализированная IDEF0-диаграмма разрабатываемого метода



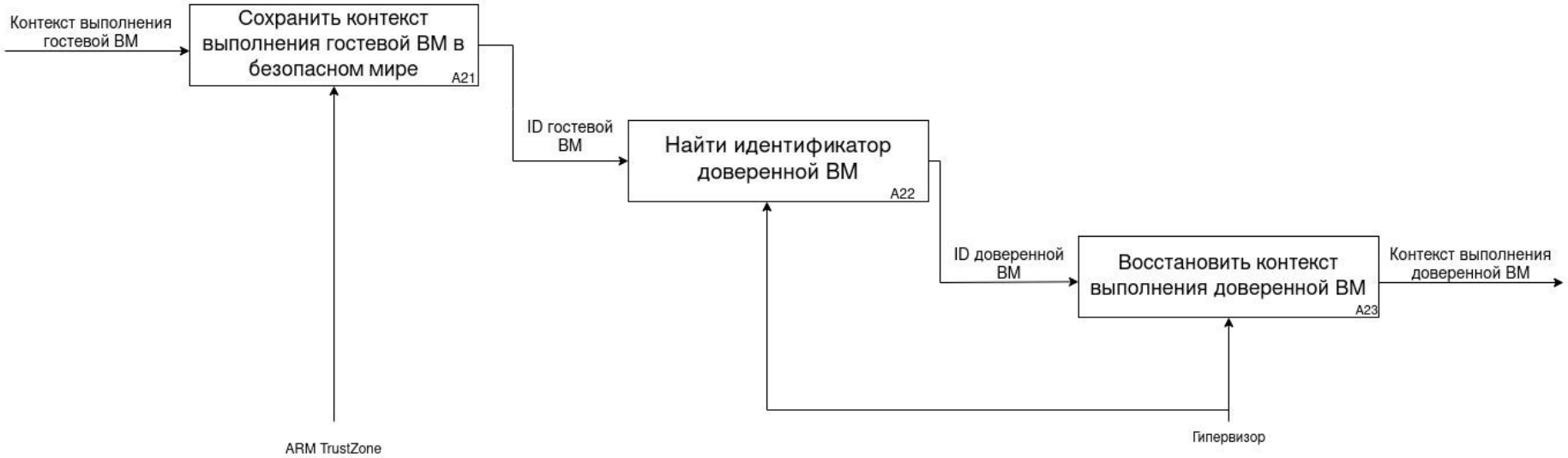
A1. Виртуализация доверенной загрузки



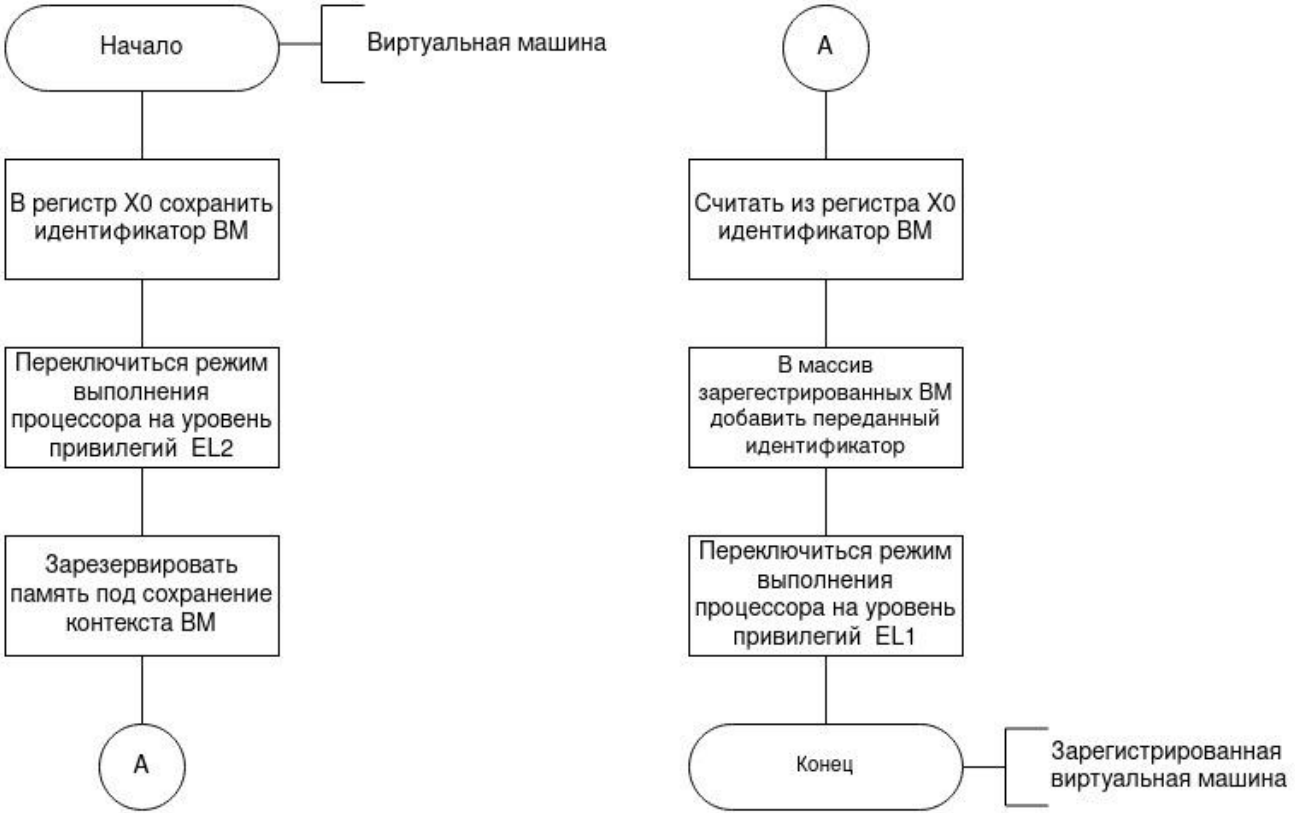
A12. Регистрация виртуальных машин



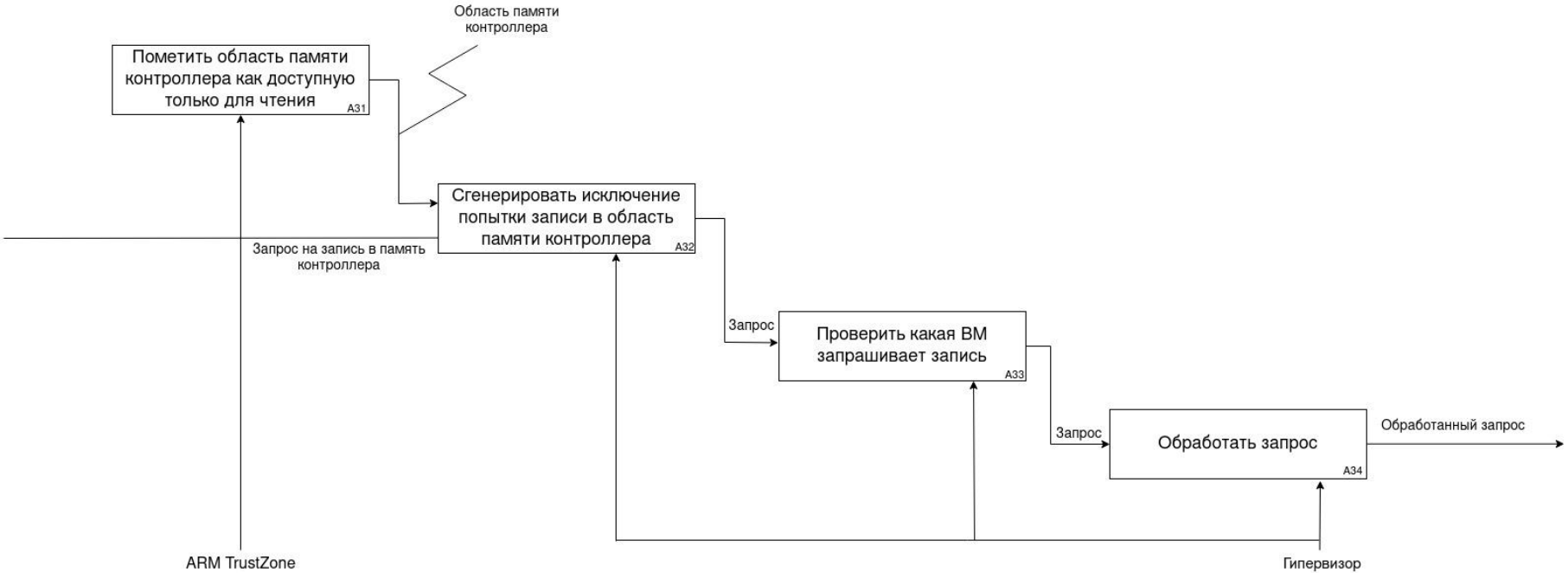
A2. Виртуализация переключения контекста



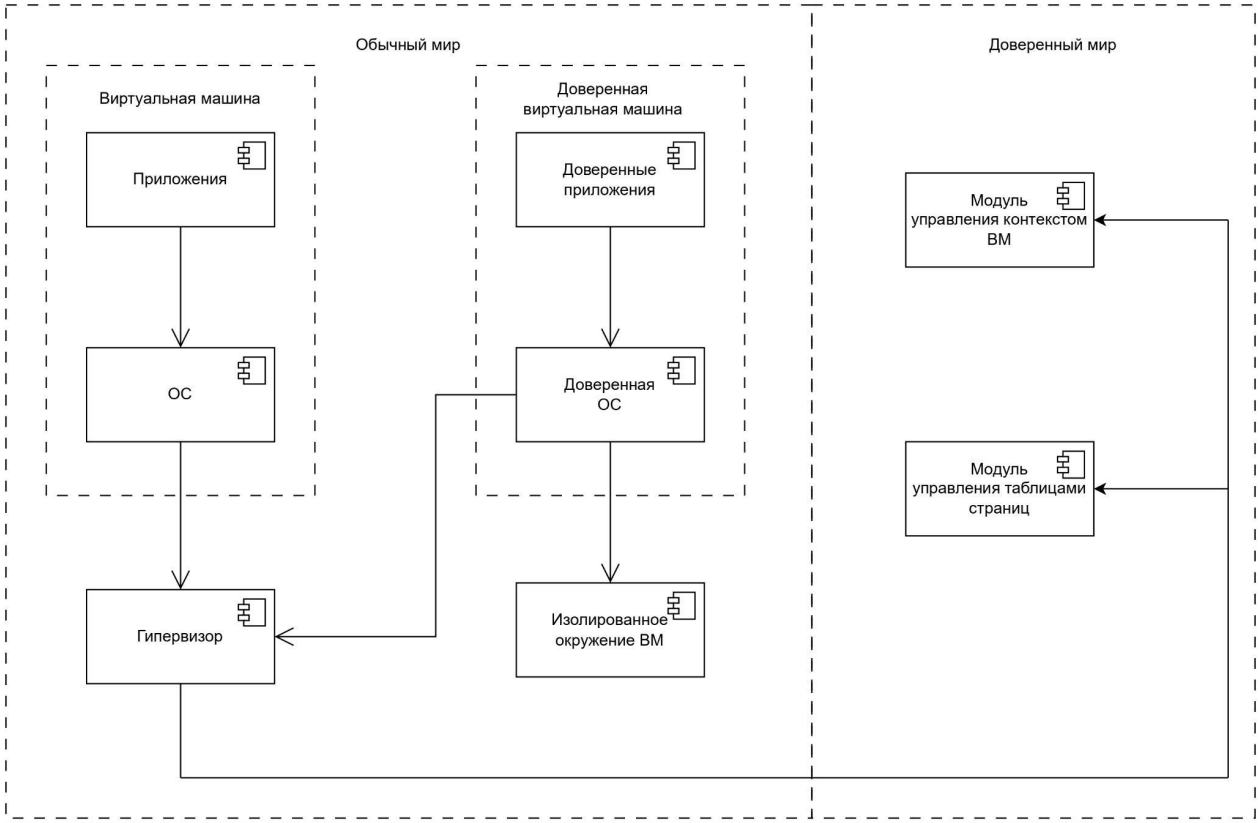
A21. Алгоритм сохранения контекста выполнения гостевой виртуальной машины



A3. Виртуализация контроллеров разделения аппаратных ресурсов



Структура программного обеспечения



Средства реализации:

- Гостевая ОС – Linux v6.9
- Доверенная ОС – OP-TEE v4.2
- Гипервизор – KVM
- Язык программирования – C (C11)

Подготовка исследования

- В качестве платформы выбран Raspberry Pi 4 Model B (ARMv8)
- Проведено сравнение быстродействия разработанного метода с аппаратной реализацией: проведено сравнение количества используемых машинных инструкций и скорости обработки операций ввода-вывода.
- Для точного подсчёта используемых машинных инструкций используется аппаратное расширение ARM Performance Unit.
- Проверена корректность разработанного метода.

Сравнение количества используемых машинных инструкций

Выполняемая операция	**Аппаратная реализация**	**Разработанный метод**
Смена контекста	1525 инструкций	7625 инструкций
Разделение участков памяти	2208 инструкций	7800 инструкций
Разделение прерываний	986 инструкций	3421 инструкций

Проверка целостности загружаемых образов ОС

Размер образа ОС	**Аппаратная реализация**	**Разработанный метод**
1 Кб	300 инструкций	325 инструкций
16 Кб	4450 инструкций	4800 инструкций
32 Кб	10200 инструкций	11223 инструкций
64 Кб	22254 инструкций	23507 инструкций
128 Кб	50700 инструкций	51998 инструкций

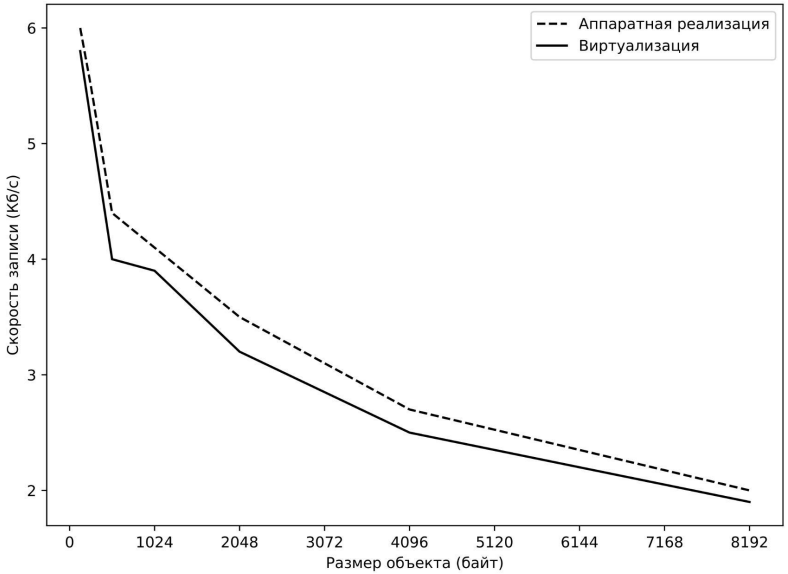
Сравнение количества используемых машинных инструкций при использовании пользовательских приложений

Шифрование файла размером 1Мб с помощью ccrypt и передача его по сети с помощью GoHttp

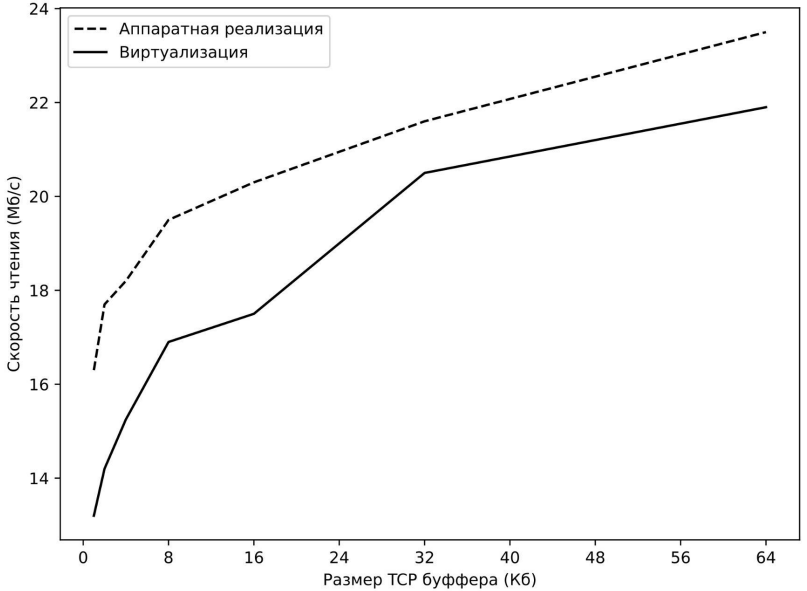
Количество пар одновременно работающих ВМ	**Аппаратная реализация**	**Разработанный метод**
1	12764 инструкций	15061 инструкций
2	15732 инструкций	22024 инструкций
4	16854 инструкций	24438 инструкций
8	17542 инструкций	26488 инструкций

Значительный рост (45-50%) используемых машинных инструкций при использовании более одной пары одновременно работающих виртуальных машин

Сравнение скорости записи и чтения при использовании серверных приложений



Зависимость скорости записи данных в СУБД MongoDB от размера объекта



Зависимость скорость чтения данных с сервера Apache от размера TCP буфера

Заключение

В результате выполнения выпускной квалификационной работы был разработан метод, реализующий программную реализацию доверенной среды исполнения с помощью виртуализации процессоров архитектуры ARM.

В процессе выполнения ВКР были выполнены следующие задачи:

- проведен анализ существующих реализаций доверенных сред исполнения
- спроектирован метод для платформ с архитектурой ARM
- спроектированы, реализованы и протестированы программные модули реализующие метод
- проведено сравнение скорости работы разработанного программного обеспечения с аппаратной реализацией.

Дальнейшее развитие

- Работа над улучшением производительности метода при использовании нескольких пар виртуальных машин одновременно