Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА - Российский технологический университет»
РТУ МИРЭА

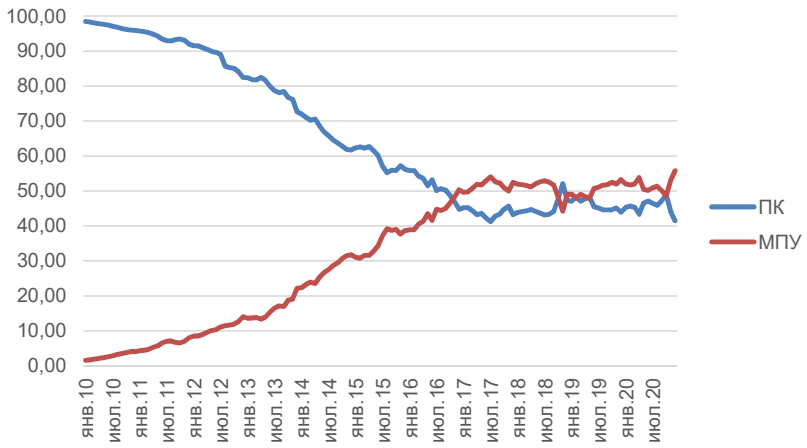
Институт комплексной безопасности и специального приборостроения
Кафедра КБ-2 «Прикладные информационные технологии»

Выпускная квалификационная работа на тему:
«Разработка сервиса поведенческого анализа функционирования мобильных устройств на операционных системах андроид»

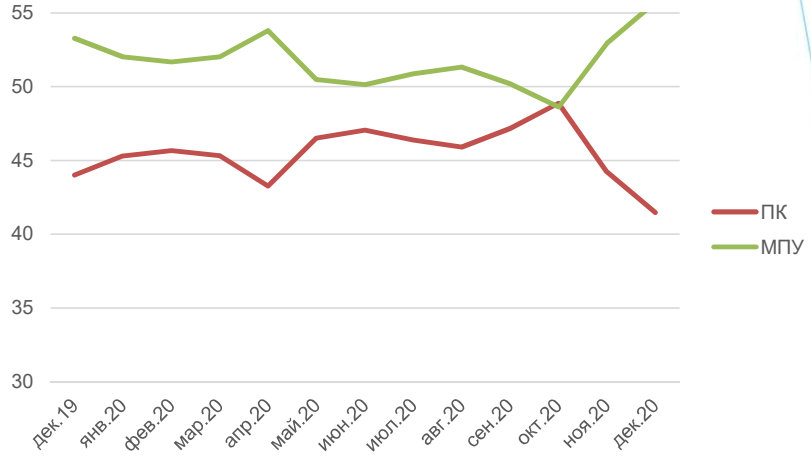
Студент: Князев Константин Антонович
Научный руководитель: Трубиенко Олег Владимирович
Научный консультант: Потерпеев Герман Юрьевич

Москва 2021

Актуальность проблемы



Темпы роста популярности ПК и МПУ в течение 10 лет



Темпы роста популярности ПК и МПУ за последний год

Уже в 2017 году мобильные устройства стали более популярными, чем персональные компьютеры и, несмотря на периодический рост и спад обоих типов устройств, заметна тенденция к увеличению популярности именно мобильных устройств.

С угрозами безопасности персональных компьютеров люди столкнулись еще в прошлом веке, а с мобильными устройствами до сих пор ситуация обстоит достаточно остро.

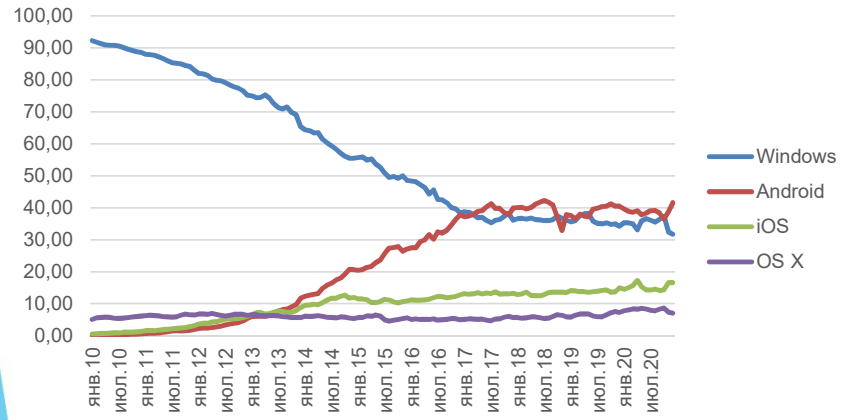
Цели и задачи

Цель работы – разработать и реализовать программное решение для реализации мониторинга устройств на операционной системе андроид.

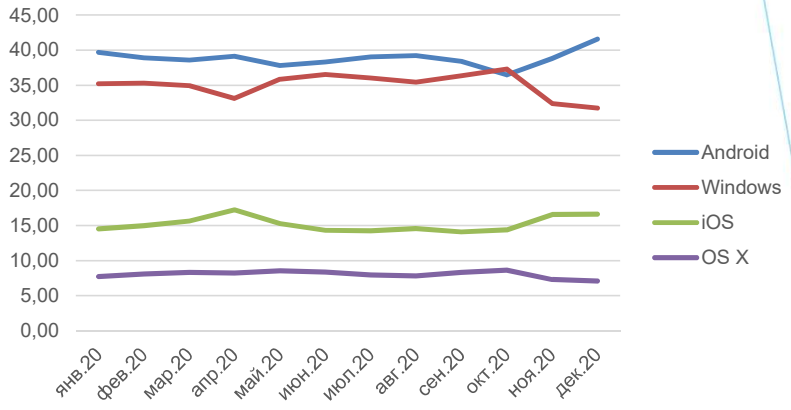
Задачи работы:

1. Провести анализ существующих ОС МПУ с последующим выбором целевой ОС;
2. Выделить набор необходимых параметров для мониторинга;
3. Провести анализ существующих средств мониторинга поведения мобильных устройств на выбранной операционной системе;
4. Реализовать средство для мониторинга функционирования мобильных устройств.

Анализ предметной области



Темпы роста популярности ОС
в течение 10 лет



Темпы роста популярности ОС
за последний год

Анализ предметной области

+ Открытый исходный код **+ Большой ассортимент устройств** **+ Большое количество приложений** **+ Гибкость интерфейса**
- Уязвимость открытой архитектуры - Оптимизация некоторых приложений

+ Направленность на пользователя **+ Оптимизация приложений** **+ Надежность закрытой архитектуры**
- Ограниченная возможность настройки - Высокая стоимость продукции - Намеренное замедление устройств

+ Схожесть с Windows 10 **+ Возможность использования некоторых приложений для Windows 10**
- Малый ассортимент устройств - Малое количество приложений - Ограниченная возможность настройки

Угрозы информационной безопасности

- Действия субъекта
- Технические средства
- Стихийные источники

Сравнение средств проведения поведенческого анализа функционирования ОС андроид

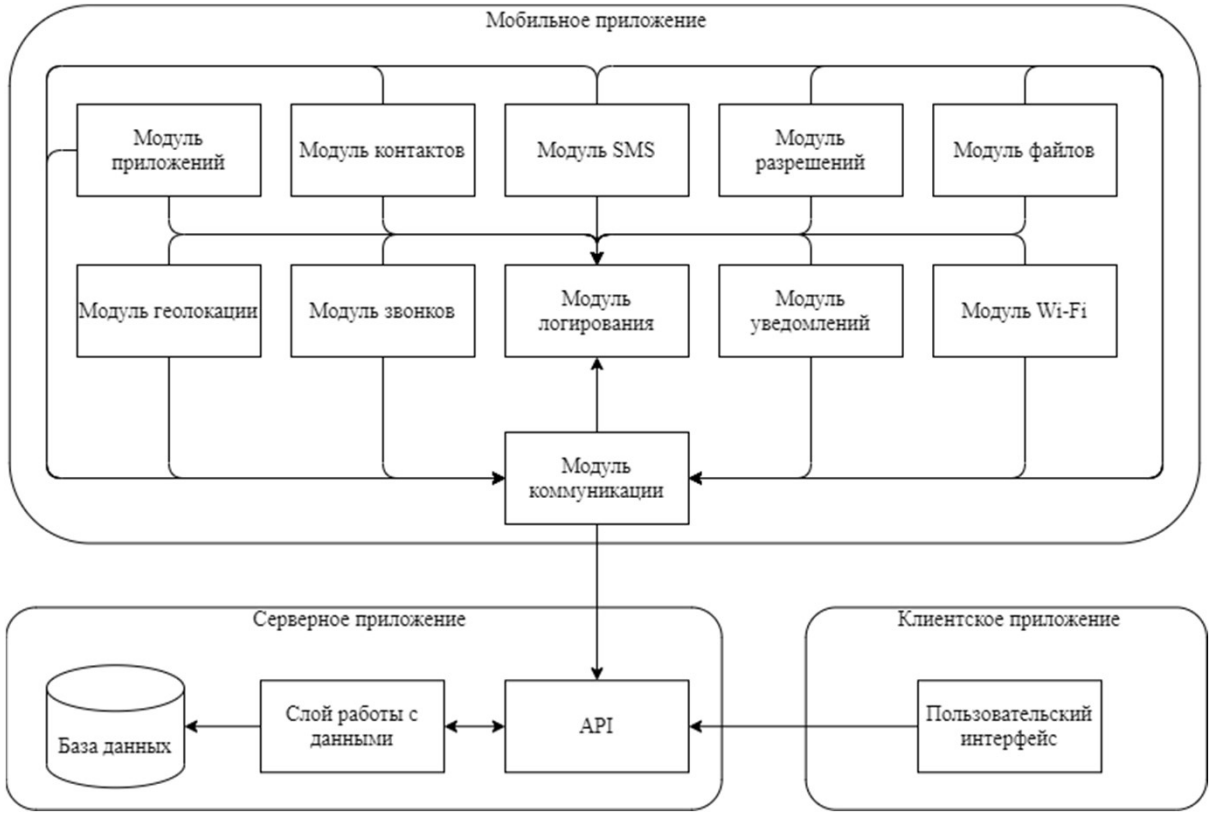
Альтернативы:

- TaintDroid
- Crowdroid
- MsfVenom

Критерии оценки:

- Работа в режиме реального времени
- Автоматизированный запуск
- Анализ действий пользователя
- Анализ на наличие вредоносного ПО
- Корректность работы
- Нейтральность для антивирусных систем
- Простота использования
- Устойчивость к нестабильному соединению
- Доступность

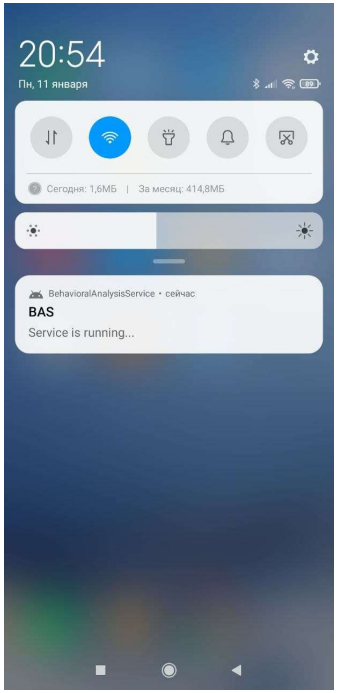
Архитектура системы

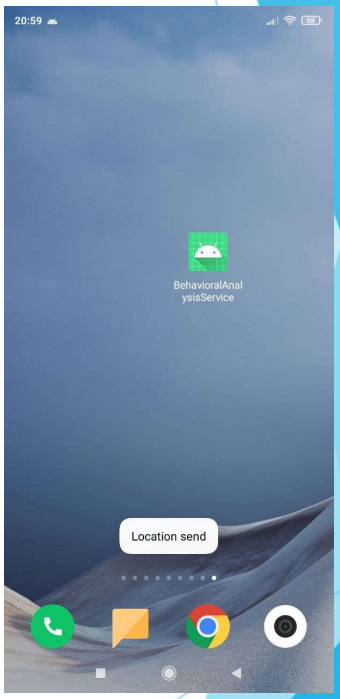


Мобильное приложение

Модули:

- Приложений
- Вызовов
- Контактов
- Геолокации
- SMS
- Wi-Fi
- Уведомлений
- Разрешений
- Файлов





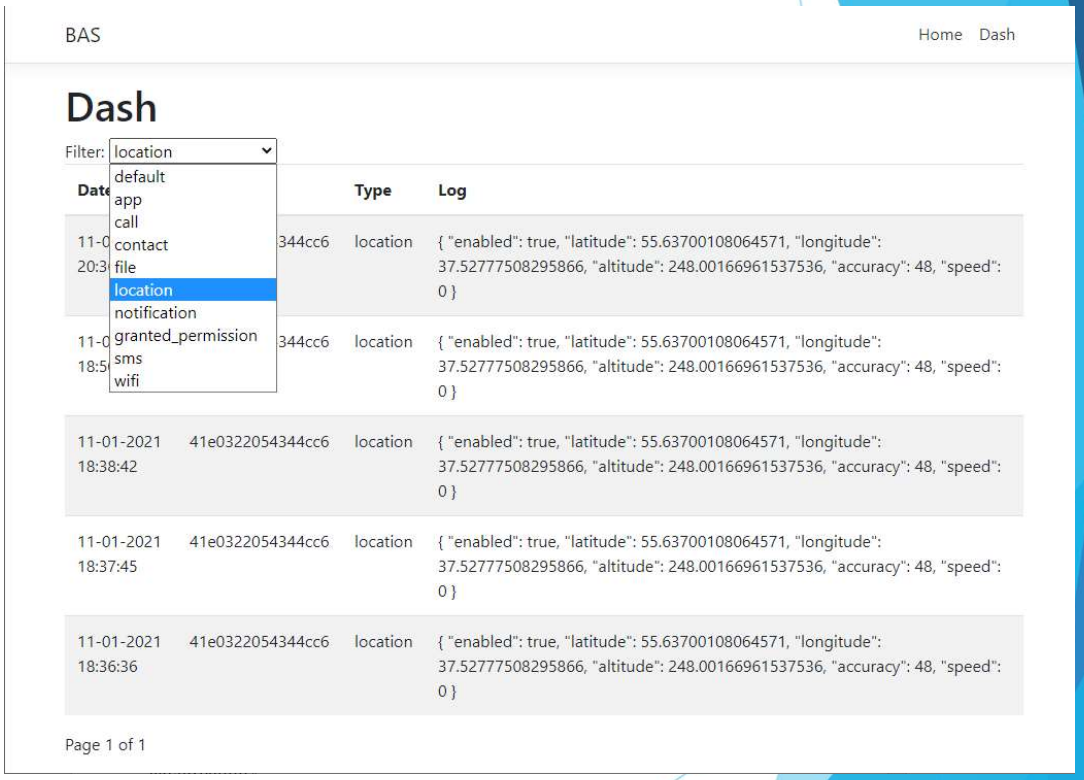
Клиент-серверная часть системы

Используемые технологии:

- .NET Core 3.1
- C#
- IIS
- Entity Framework Core
- Sql Server
- React
- Redux

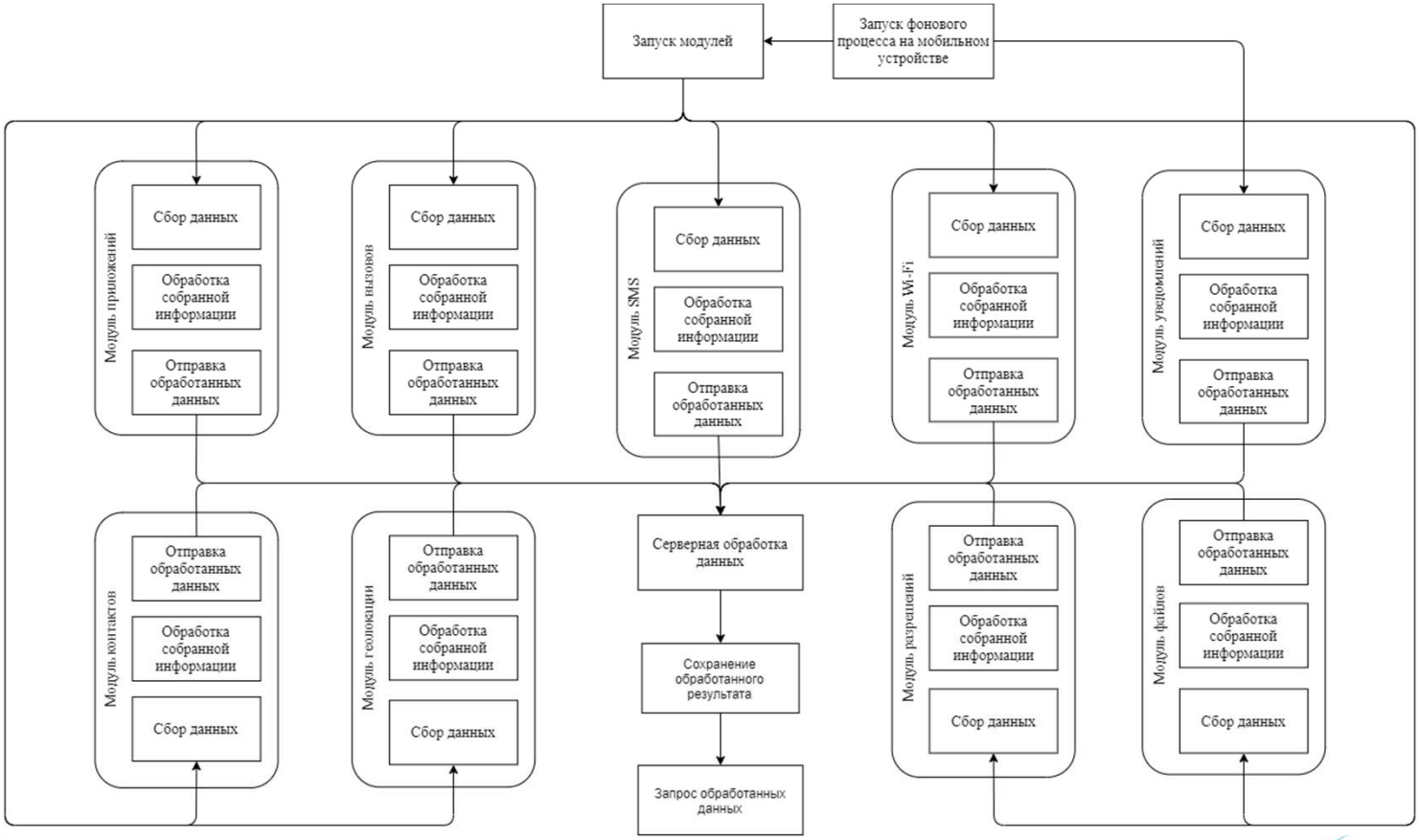
Log			
PK	Id Guid NOT NULL		
	DeviceId	varchar(max)	NOT NULL
	Type	int	NOT NULL
	Created	date	NOT NULL
	Value	varchar(max)	NOT NULL

Таблица логов



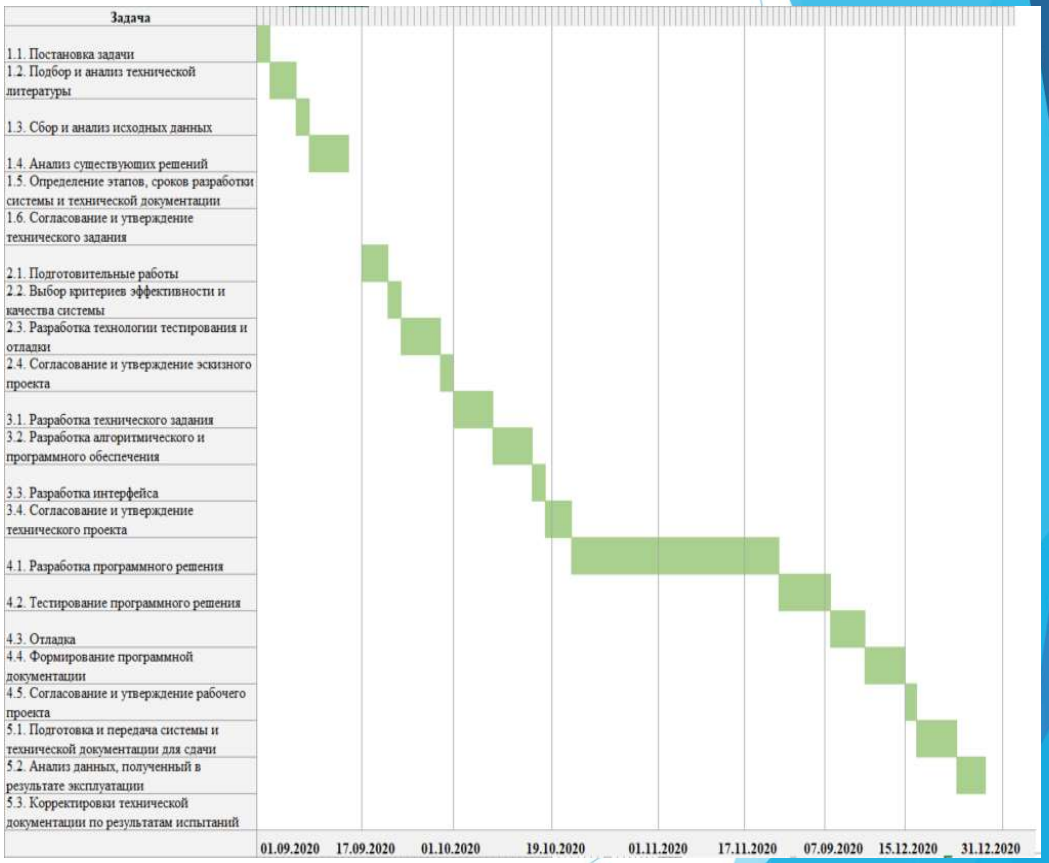
Панель для анализа данных

Алгоритм работы системы



Экономическое обоснование

Статья затрат	Обозначение	Величина затрат (руб.)	% затрат к итогу
Затраты на основные материалы	$C_{мат}$	1345.00	0.29%
Основная заработная плата	$C_{осн}$	222956.00	47.40%
Дополнительная заработная плата	$C_{доп}$	33443.40	7.11%
Отчисления от заработной платы	$C_{отч}$	76919.90	16.35%
Накладные расходы	$C_{накл}$	133773.80	28.44%
Машинное время	$C_{м.вр}$	1963.44	0.42%
Итого	$C_{разр}$	470401.54	100,00%



Выводы

- Выделены наиболее популярные мобильные ОС
- Выделен набор необходимых для мониторинга параметров
- Проведен анализ существующих средств проведения поведенческого анализа работы ОС андроид
- Реализован сервис мониторинга функционирования мобильной ОС андроид