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

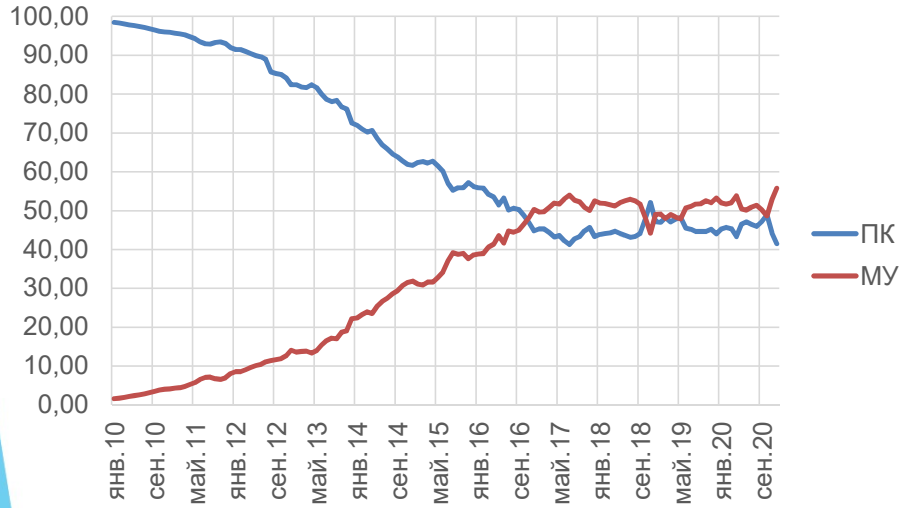
Институт комплексной безопасности и специального приборостроения
Кафедра КБ-2 «Прикладные информационные технологии»

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

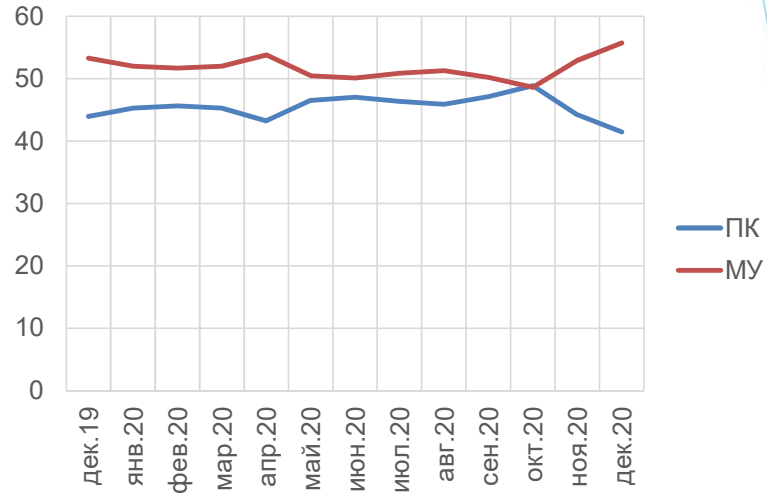
Выполнил: студент Князев Константин Антонович
Научный руководитель: к.т.н., доцент Трубиенко Олег Владимирович
Научный консультант: к.т.н., доцент Потерпеев Герман Юрьевич

Москва, 2021

Актуальность проблемы



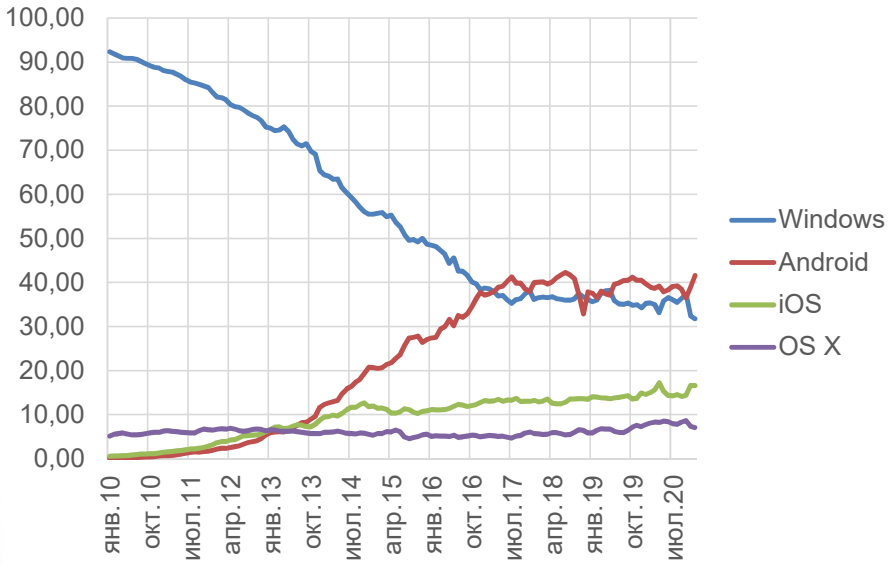
Темпы роста популярности ПК и МУ в течение 10 лет



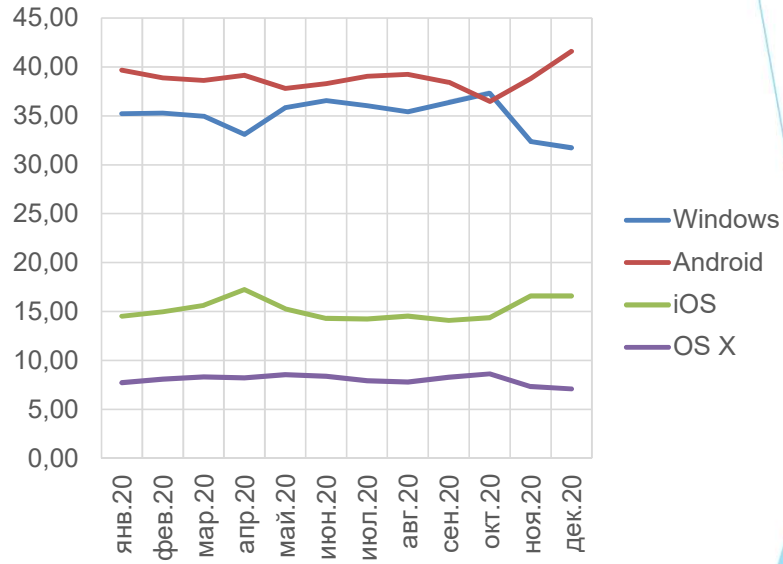
Темпы роста популярности ПК и МУ за последний год

statcounter

Актуальность проблемы



Темпы роста популярности ОС в течение 10 лет



Темпы роста популярности ОС за последний год

statcounter

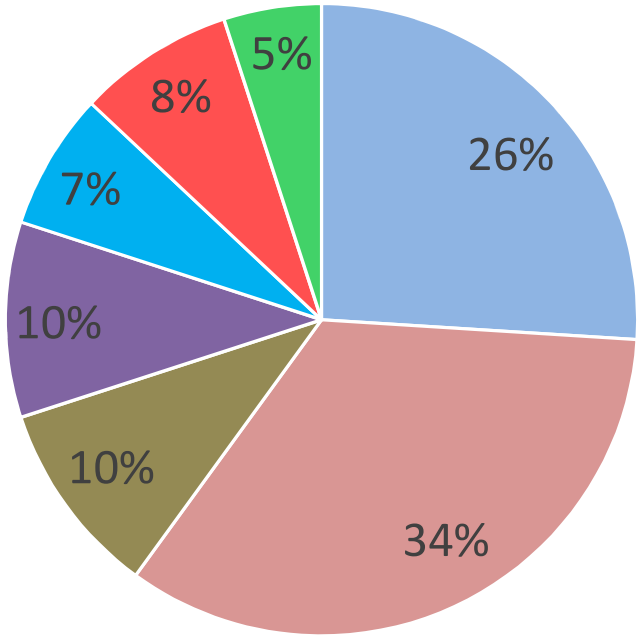
Цели и задачи

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

Задачи работы:

1. Провести анализ существующих ОС МУ 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.

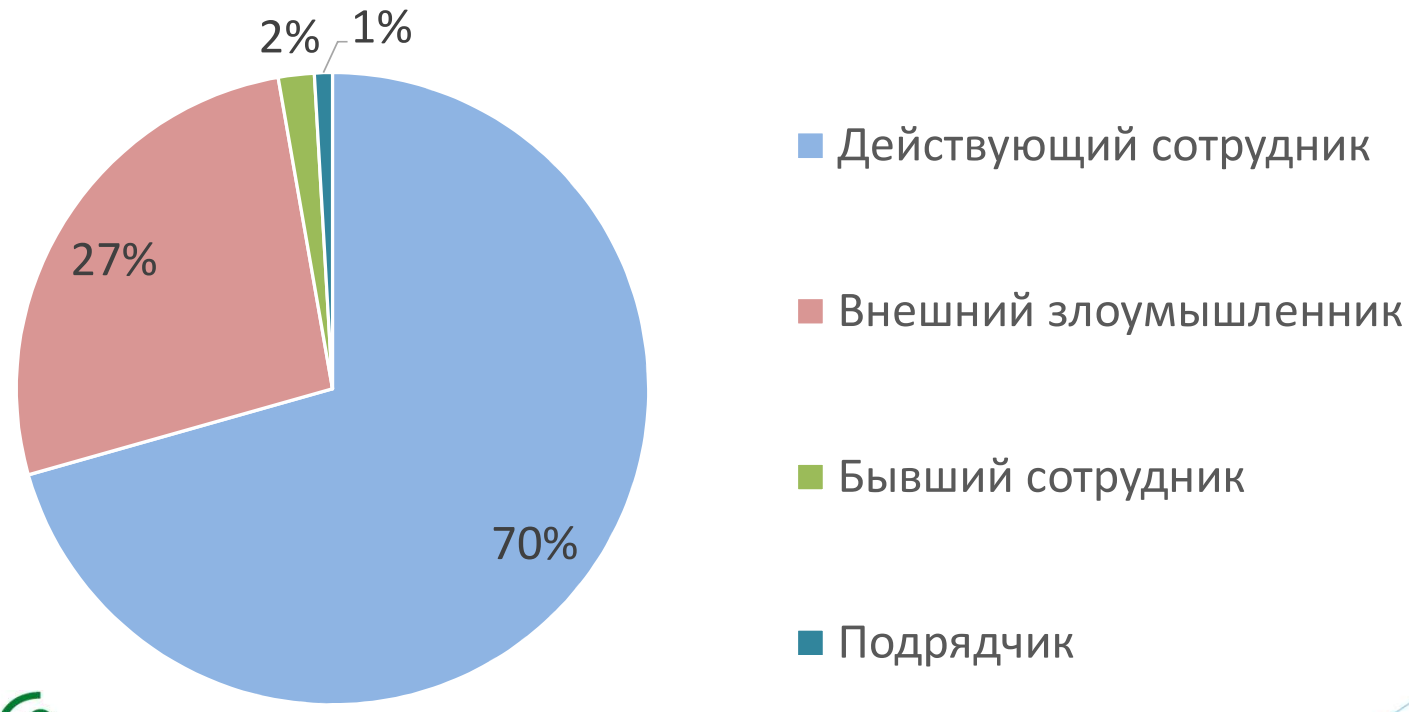
Угрозы информационной безопасности в компании



- Вирусы
- Действия сотрудников, фишинг, инсайдеры
- DDoS атаки
- Кража оборудования
- Криптеры
- Таргетированная атака
- Эксплойты

KASPERSKY lab

Источники утечки информации в корпорации



INFOWATCH®

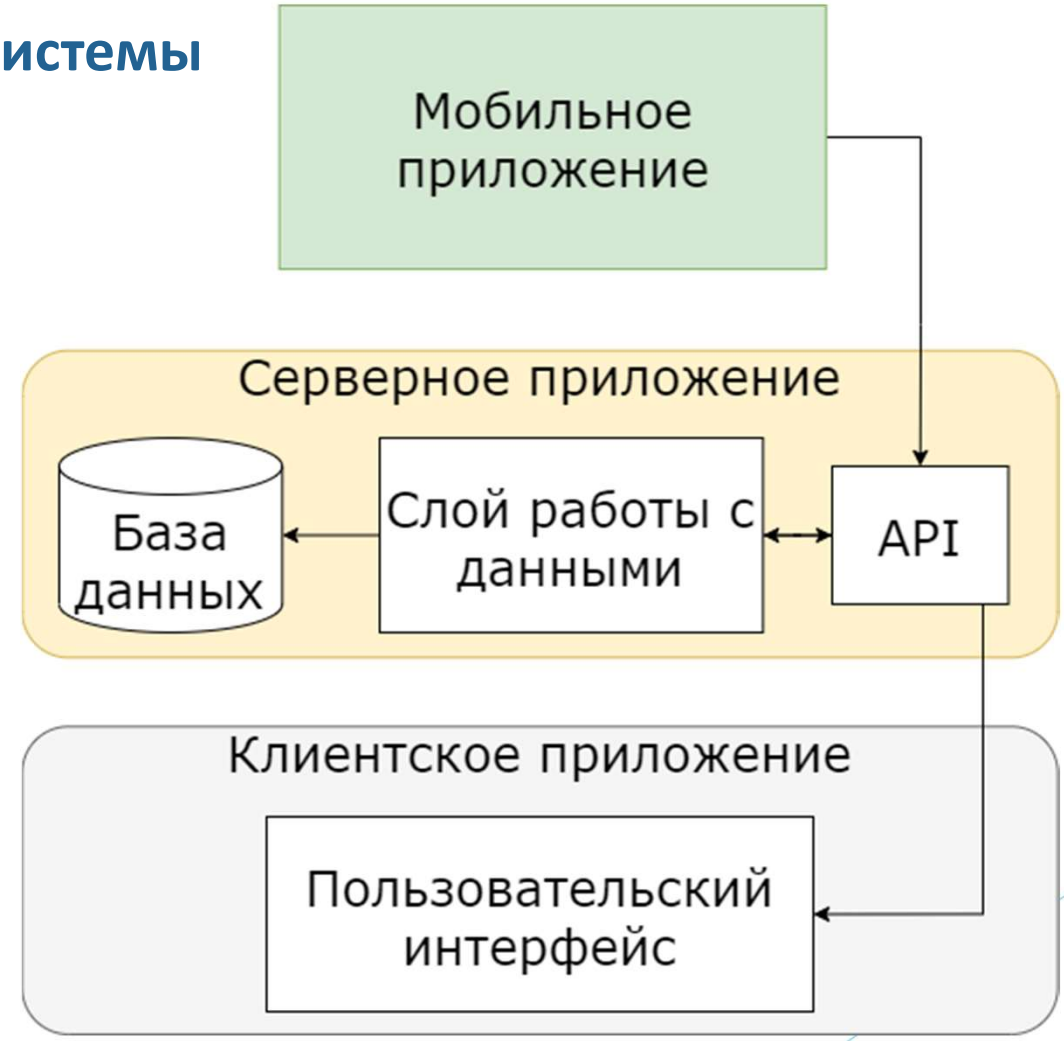
Риски, которые несут инсайдеры

- Украсть конфиденциальную информацию и передать ее конкурентам
- Обнародовать персональные данные, попадающие под действие государственных регламентов
- Уничтожить информацию, критически важную для работы компании
- Установить и запустить вредоносное программное обеспечение.
- Отключить или вывести из строя ИБ-системы

Сравнение средств поведенческого анализа мобильных устройств на операционной системе андроид

	Автоматизированная работа в режиме реального времени	Устойчивость к нестабильному соединению	Анализ действий пользователя
TaintDroid	-	+	+
CrowDroid	+	+	-
MsfVenom	-	-	-

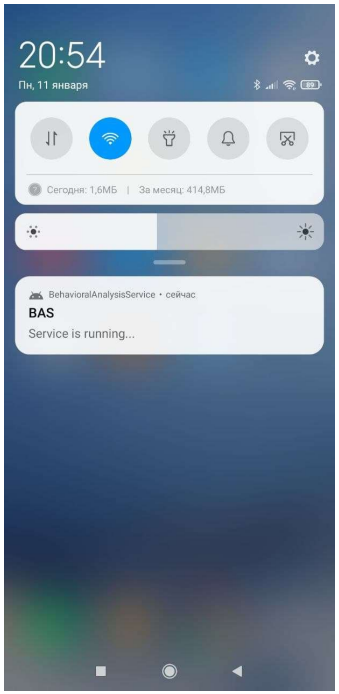
Архитектура системы

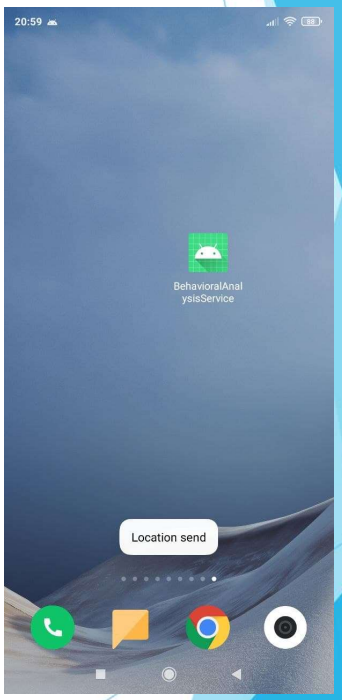


Мобильное приложение

Модули:

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





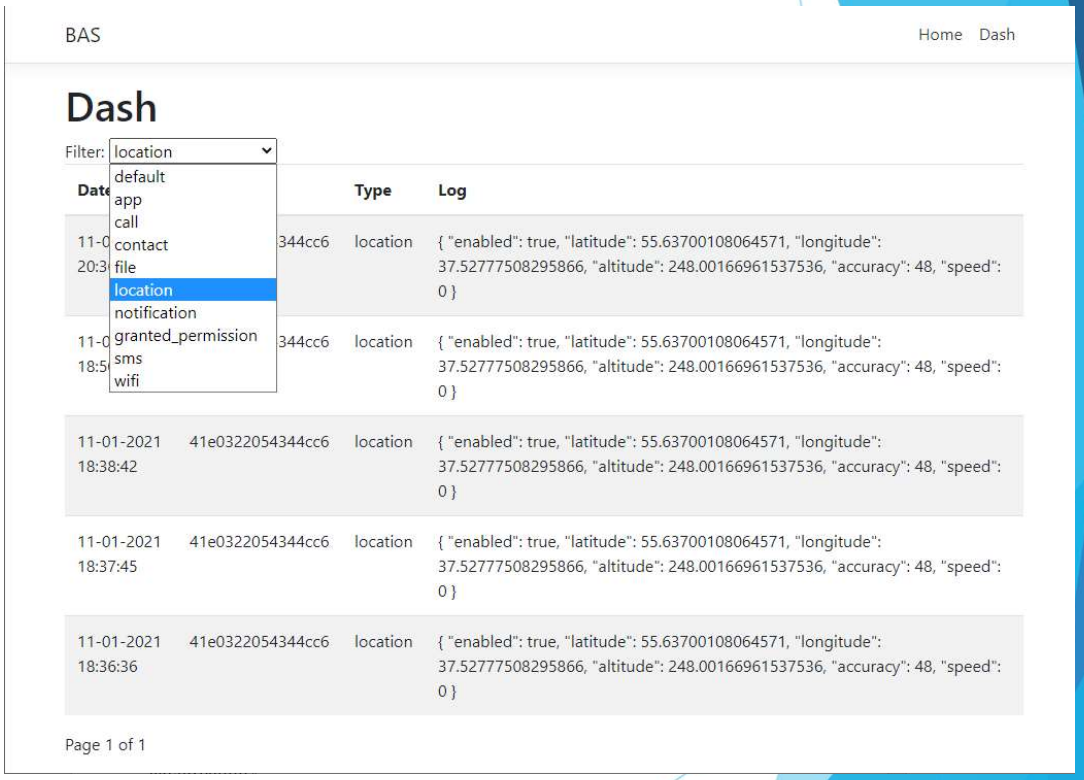
Клиент-серверная часть системы

Используемые технологии:

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

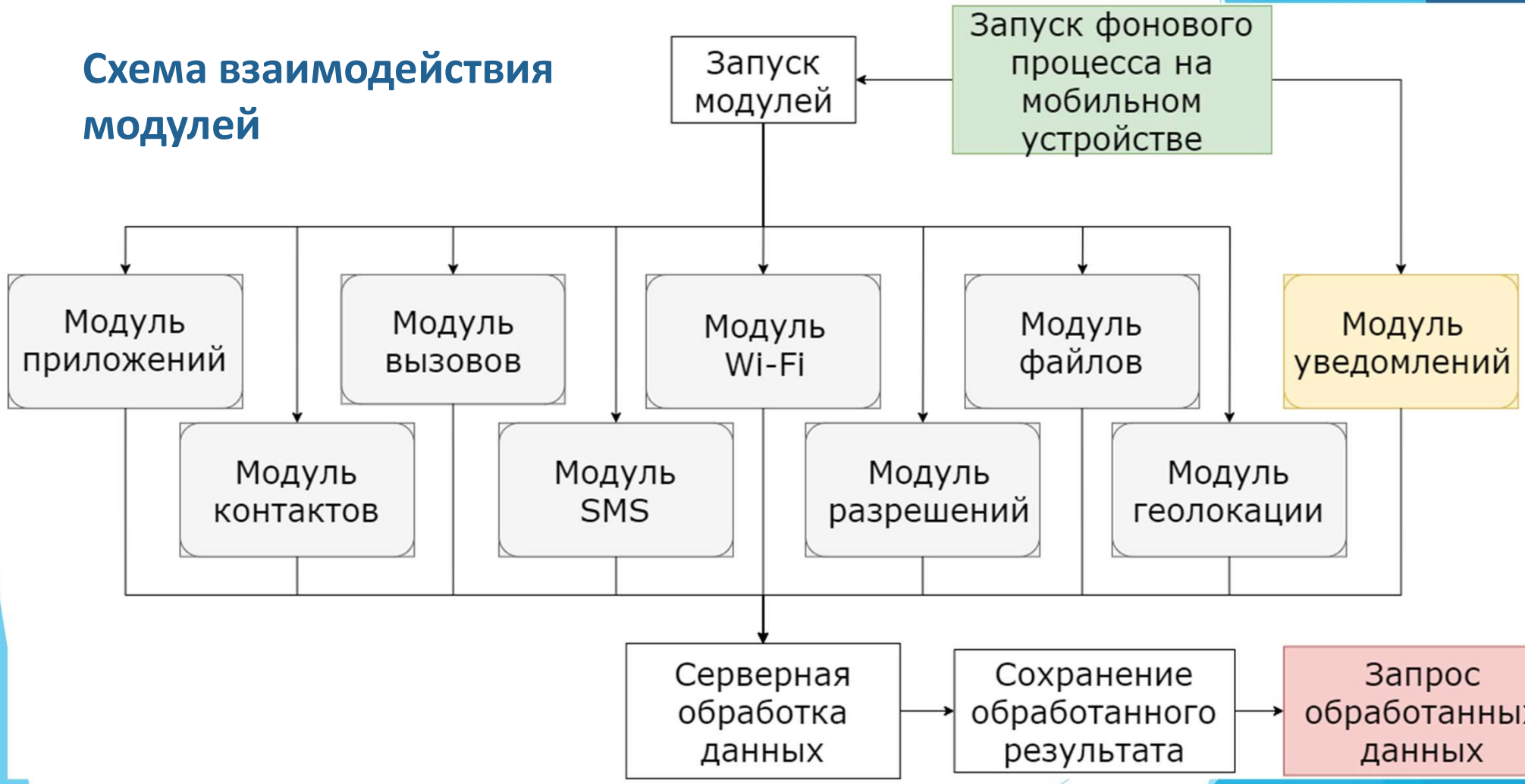
Log			
PK	Id Guid NOT NULL		
	DeviceId	varchar(max)	NOT NULL
	Type	int	NOT NULL
	Created	date	NOT NULL
	Value	varchar(max)	NOT NULL

Таблица логов



Панель для анализа данных

Схема взаимодействия модулей



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

Спасибо за внимание!