

«Использование облачной платформы аутентификации по подписи при создании защищённого мобильного приложения»

Выполнил

Пасенчук Виктор Андреевич,

Научный руководитель

Ложников Павел Сергеевич

Актуальность работы

- Ограничение доступа, основанное на использовании некоего мастер-пароля или токена, а также хранение в сейфе имеет недостаток: отделимость аутентификатора доступа к хранилищу от владельца.
- Из этого следует, что для повышения надёжности хранения информации возможно использовать неотделимые от хозяина признаки, то есть его биометрические данные.
- Простым и удобным для распознавания мобильными устройствами биометрическим признаком является анализ рукописного ввода.

Цель работы

- Целью данной работы является создание альтернативы существующим методам аутентификации, используемым в мобильных устройствах, использующей в качестве аутентификатора ввод рукописного пароля.

Задачи

Для достижения цели требуется выполнить следующие задачи:

1. Анализ рынка систем биометрической аутентификации;
2. Сравнение существующих систем аутентификации по рукописному паролю;
3. Анализ особенностей системы SignToLogin;
4. Разработка архитектуры сервиса;
5. Создание библиотеки SignToLogin SDK, позволяющей использовать аутентификацию по подписи при создании мобильных приложений;
6. Разработка мобильного приложения SignPass на основании SignToLogin SDK;
7. Публикация созданного приложения в Google Play;
8. Сбор аналитики использования приложения;

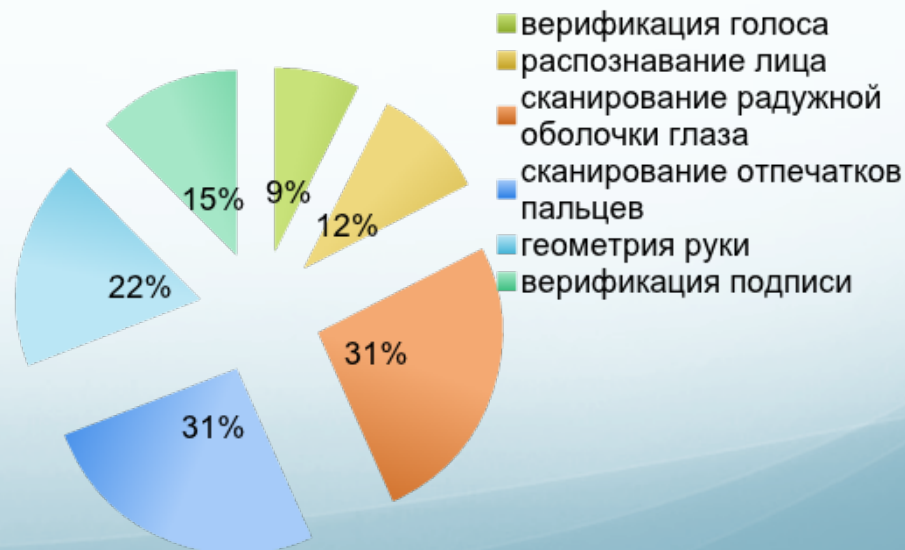
1. Анализ рынка систем биометрической аутентификации

Мировой рынок биометрических систем **\$7,3 млрд.** из них на **верификацию подписи \$226 млн.** в 2013 г. с перспективой роста **35%** в год. Годовой оборот почерковедческих бюро составляет **44,6 млн. руб.**

ОСНОВНЫЕ ПОТРЕБИТЕЛИ

- Промышленные предприятия
- Банки
- Объекты стратегического назначения
- Торговые организации

Рынок биометрических систем



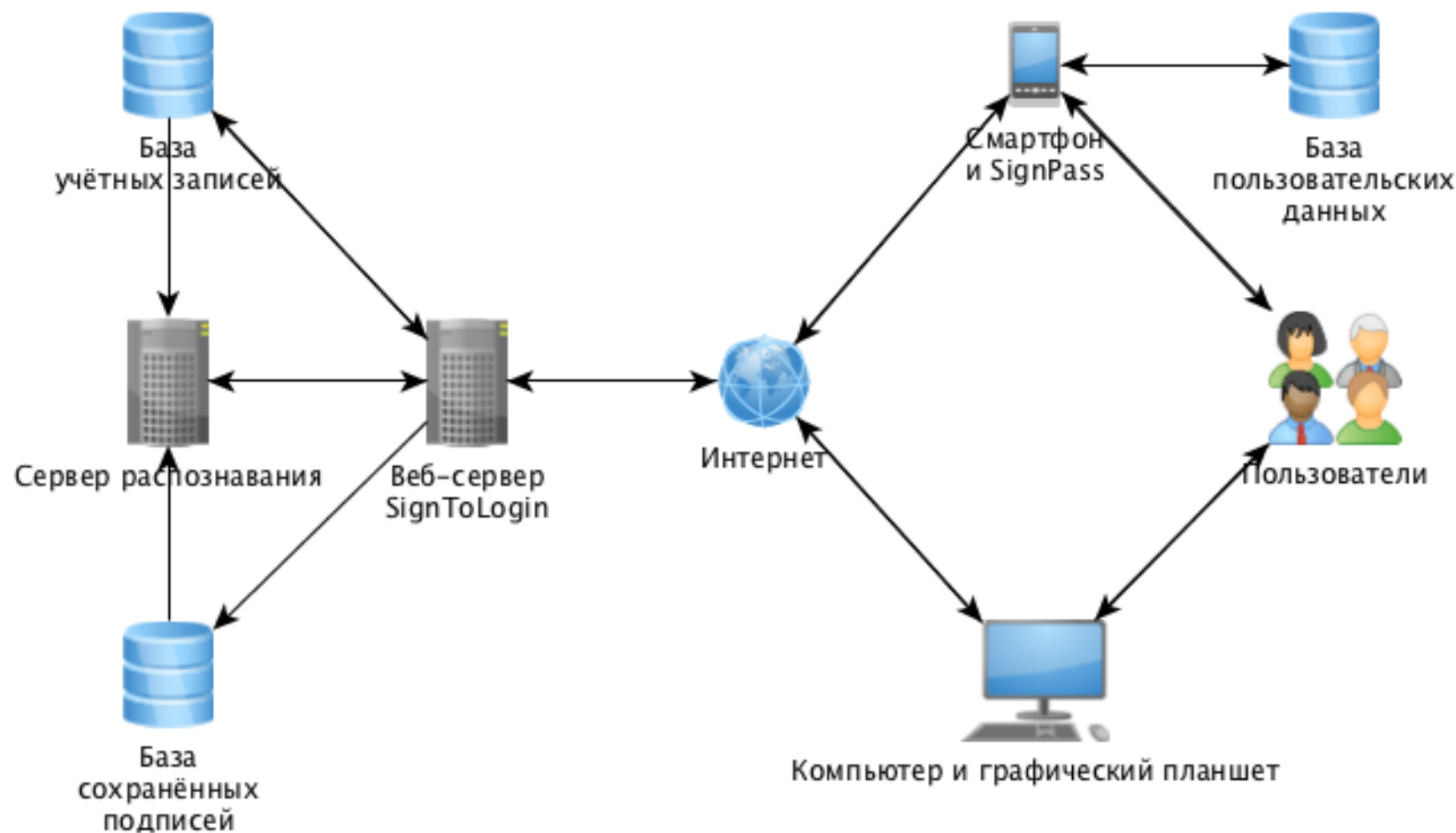
2. Сравнение системы распознавания подписи SignToLogin с аналогами

Характеристики	SignToLogin	CIC	SignDocDesktop
Не обязательное использование графического планшета	+	-	+
Анализ статического изображения подписи	-	-	-
Поддержка мобильных устройств	+	-	+
Анализ документов	-	-	-
Использование формы	+	+	+
Использование размера	+	+	+
Использование наклона	+	+	+

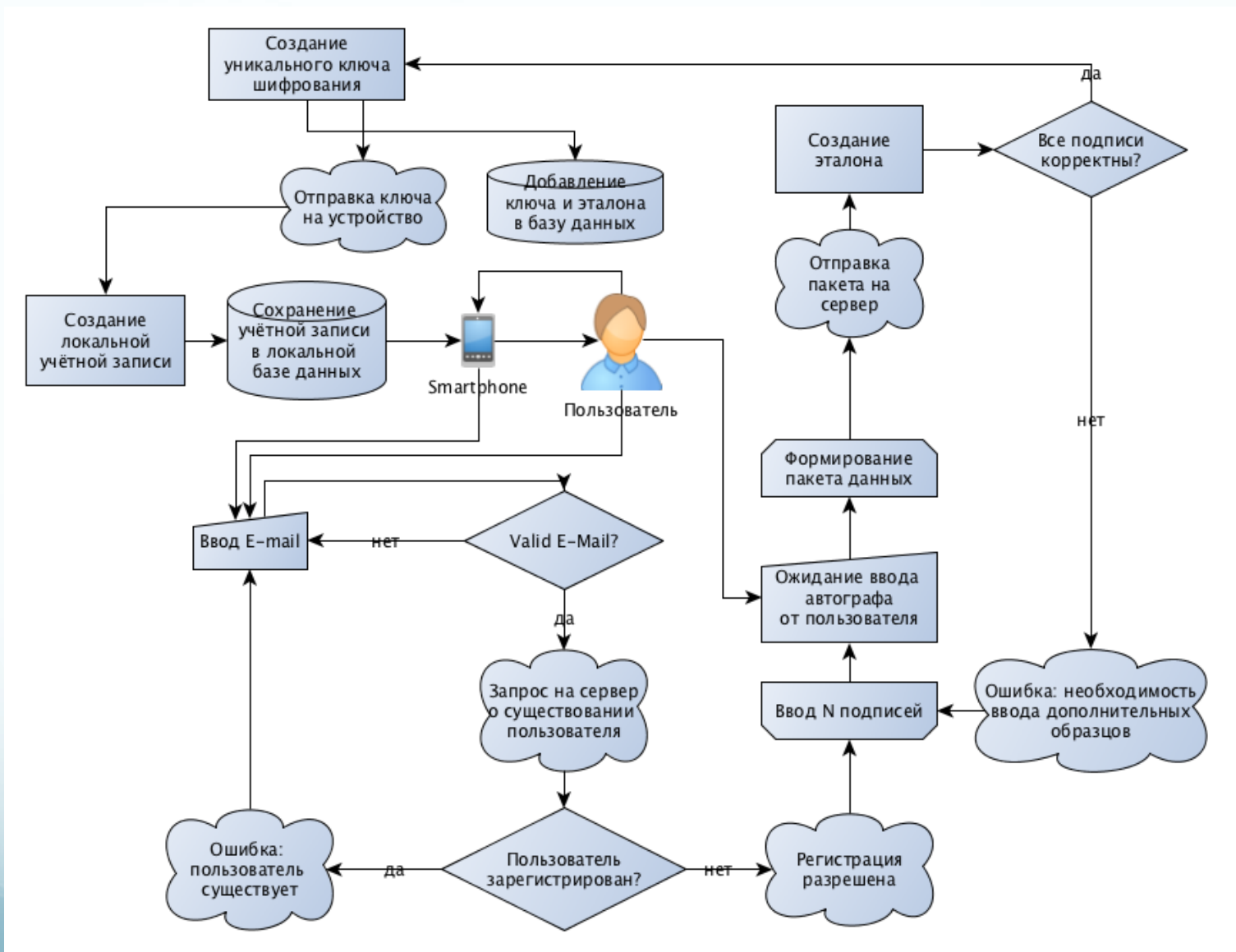
3. Анализ особенностей системы SignToLogin

- Сравнение введённой подписи с созданным образцом проводится по методике, разработанной в НТЦ «Касиб». Согласно данной методике, сопоставление автографов осуществляется не по соответствию графического изображения, а по динамике написания подписи, которая в свою очередь напрямую связана с индивидуальными когнитивными процессами каждого человека.
- Для того, чтобы определить, является ли субъект аутентифицированным пользователем, требуется сравнить его автограф с зарегистрированным ранее эталоном. Для получения эталонного набора требуется ввод не менее 10 образцов подписи. В случае, если некоторые образцы имеют существенные отличия от прочих, требуется повторный ввод спорных образцов.
- Сумма вероятностей ошибок первого и второго рода составляет 2%.

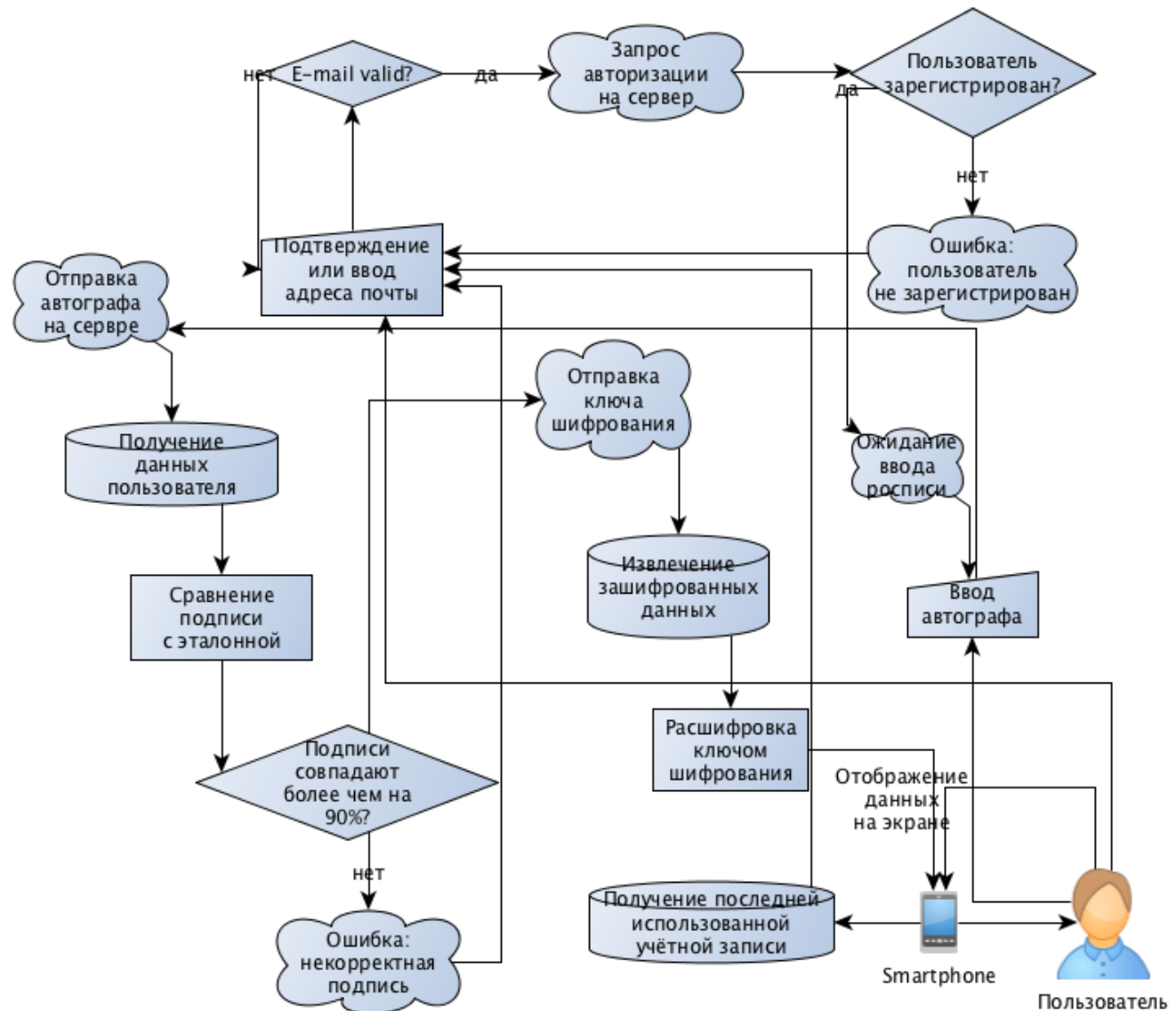
4.1 Разработка концептуальной схемы взаимодействия узлов



4.2 Разработка протокола регистрации



4.3 Разработка протокола авторизации



Недостатки архитектуры

Стремление минимизировать угрозу попадания конфиденциальных данных третьим лицам привело к возникновению ряда недостатков:

- Отсутствует возможность синхронизации данных с помощью облачных сервисов.
- При утере или повреждении устройства данные также будут потеряны.
- В случае травмы руки, которой осуществляется роспись, будет утеряна способность корректно ввести подпись. Таким образом, пользователь может потерять возможность доступа к своим данным.
- Приложение требует доступа к Интернет для проверки подписи. Без доступа к Интернет пользователь не сможет получить ключ шифрования и просмотреть свои данные.

5. SignToLogin SDK for Android

- Библиотека для Android OS.
- Собрана в виде jar файла.
- Позволяет использовать сервис SignToLogin в сторонних приложениях.
- Содержит инструменты для использования возможностей онлайн-сервиса SignToLogin.
- Содержит SignView, которая обладает необходимым функционалом для отображения, фиксирования и сохранения подписи.
- Совместимость с Android OS версии 1 и выше (API level 1 and above).

6.1 Инструменты разработки

- SignToLogin SDK for Android.
- IDE: Android Studio.
- Build system: gradle.
- Libs: otto, butterknife, gson, sql assets helper, appcompat.
- Analytics: crashlytics, crashlytics answers.
- Fast deploy: crashlytics beta.

6.2 Разработка алгоритма безопасного хранения конфиденциальной информации в мобильном приложении

- Безопасность сервиса обеспечивается следующими факторами:
- Используемая размерность ключа шифрования (256 бит) является достаточной для защиты от полного перебора в абсолютном большинстве случаев.
- Используемый алгоритм шифрования AES не имеет уязвимостей для основных видов криптоатак.
- Использование режима шифрования CBC/PKCS5Padding гарантирует, что одинаковые блоки данных отобразятся в разные блоки шифртекста.
- Конфиденциальные данные хранятся только на устройстве в зашифрованном виде.
- Как сервер SignToLogin, так и устройство (в момент, когда приложение не активно) не обладают достаточным набором информации для расшифровки данных. Таким образом, в случае кражи или утери устройства, злоумышленник не сможет получить доступ к конфиденциальной информации.

6.3 Реализация безопасного соединения с сервером распознавания подписей

- Вся коммуникация с SignToLogin осуществляется через зашифрованный канал по протоколу HTTPS. Подлинность сертификатов SSL может быть подтверждена организацией Thawte, Inc.
- Платформа SignToLogin была специально доработана для оптимальной и безопасной работы SignPass

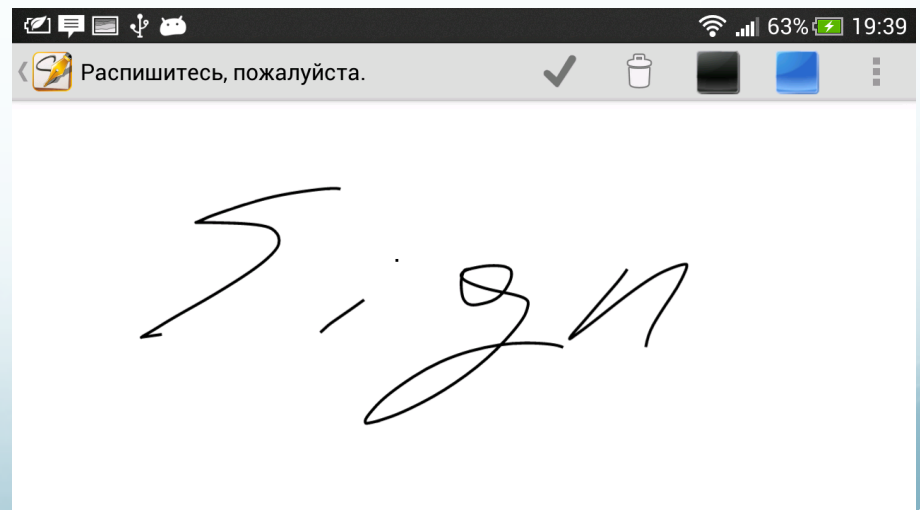
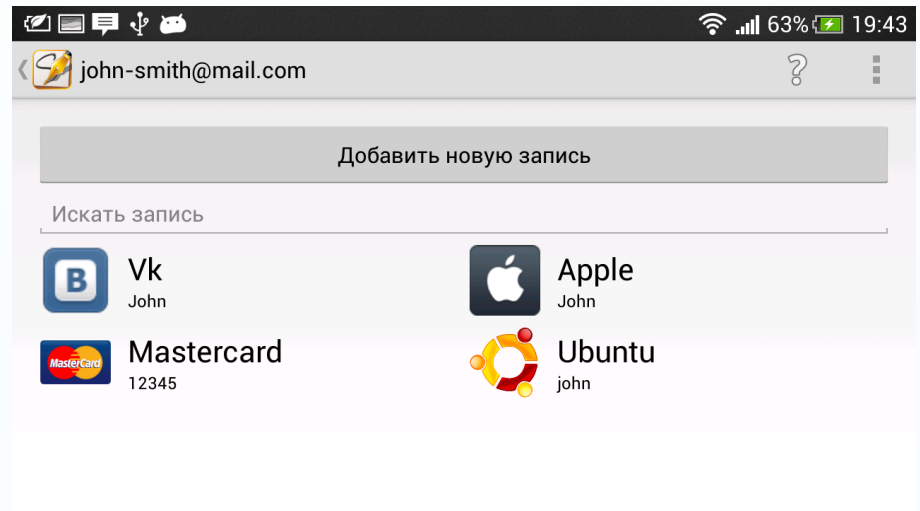
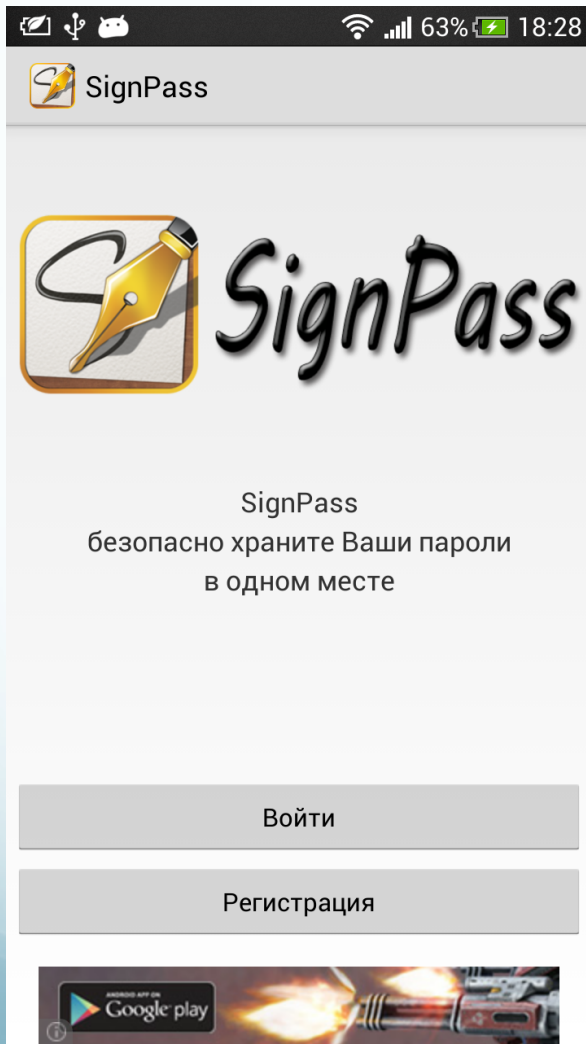
6.4 Разработка пользовательского интерфейса, обеспечивающего высокий уровень безопасности и эргономичности

- Аутентификация с использованием автографа.
- Возможность иметь несколько учётных записей на одном устройстве.
- Широкий перечень сервисов, для которых можно сохранить учётные данные. Для обеспечения удобства пользователя в приложении содержится большое количество пиктограмм для различных сервисов.
- Создание, просмотр, редактирование, удаление записей.
- Копирование аутентифицирующей информации в буфер обмена. Возможность отображения паролей на экране (из соображений безопасности данное действие требует подтверждение пользователя).
- Существует отключаемый строгий режим повышенной безопасности, при котором переход приложения в неактивное состояние (сворачивание, полное перекрытие другим приложением, отключение экрана устройства) ведёт к автоматическому выходу из текущей учётной записи.

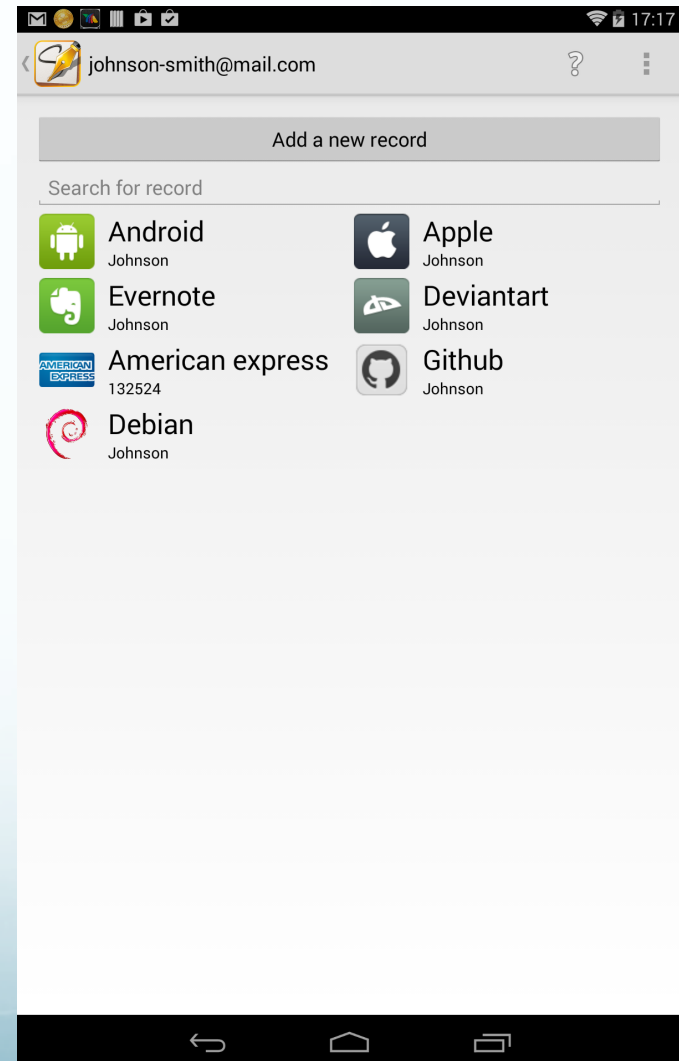
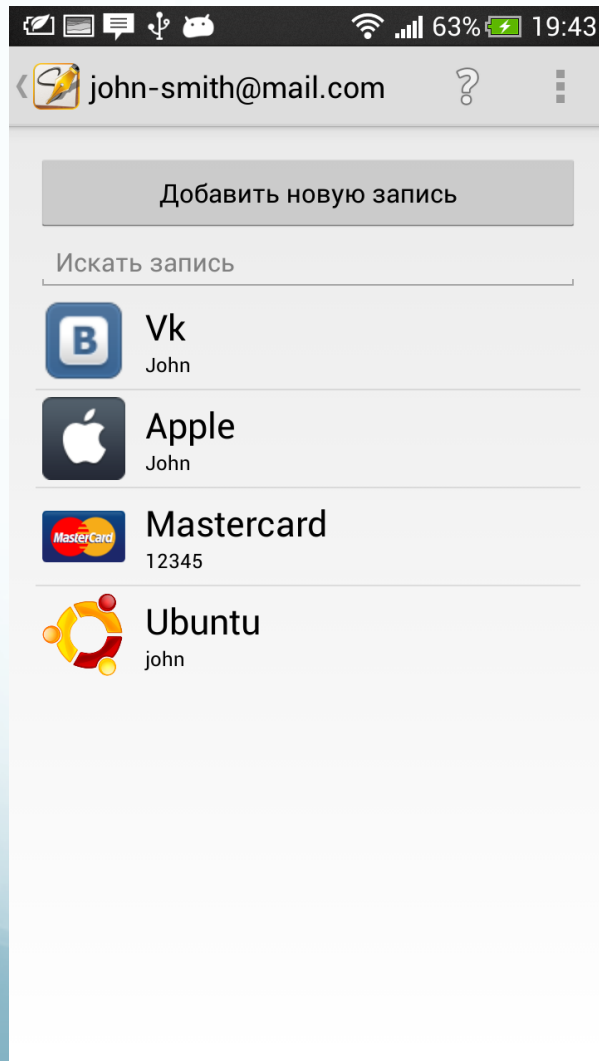
6.5 Оптимизация приложения для различных устройств

- Поддержка различных конфигураций и размеров экрана.
- Наличие русской и английской локализации.
- Возможности настройки отображения подписи.

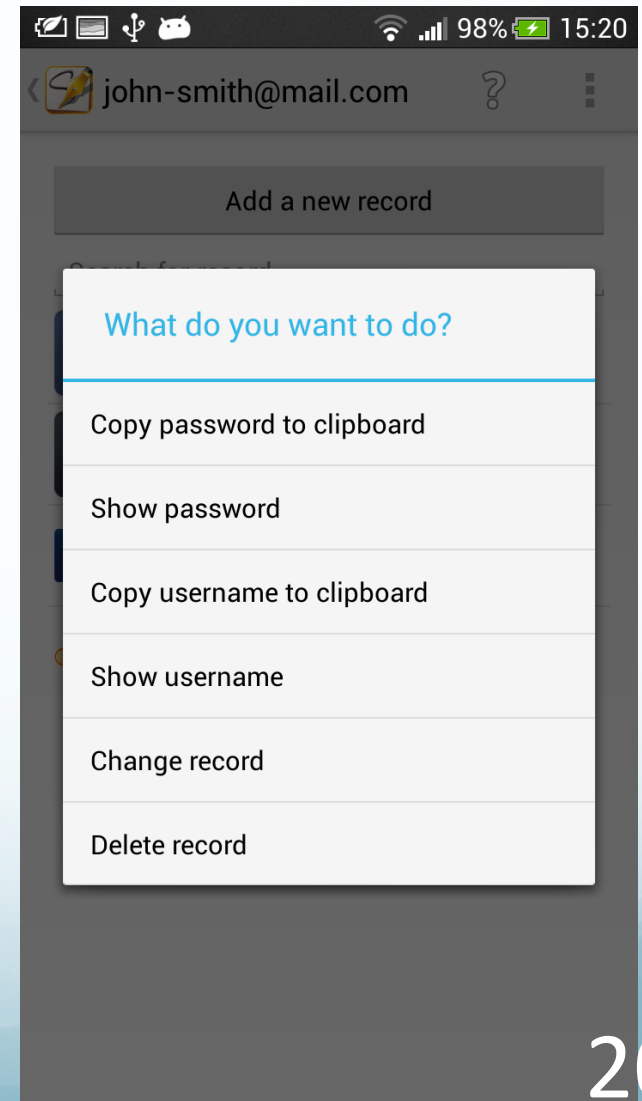
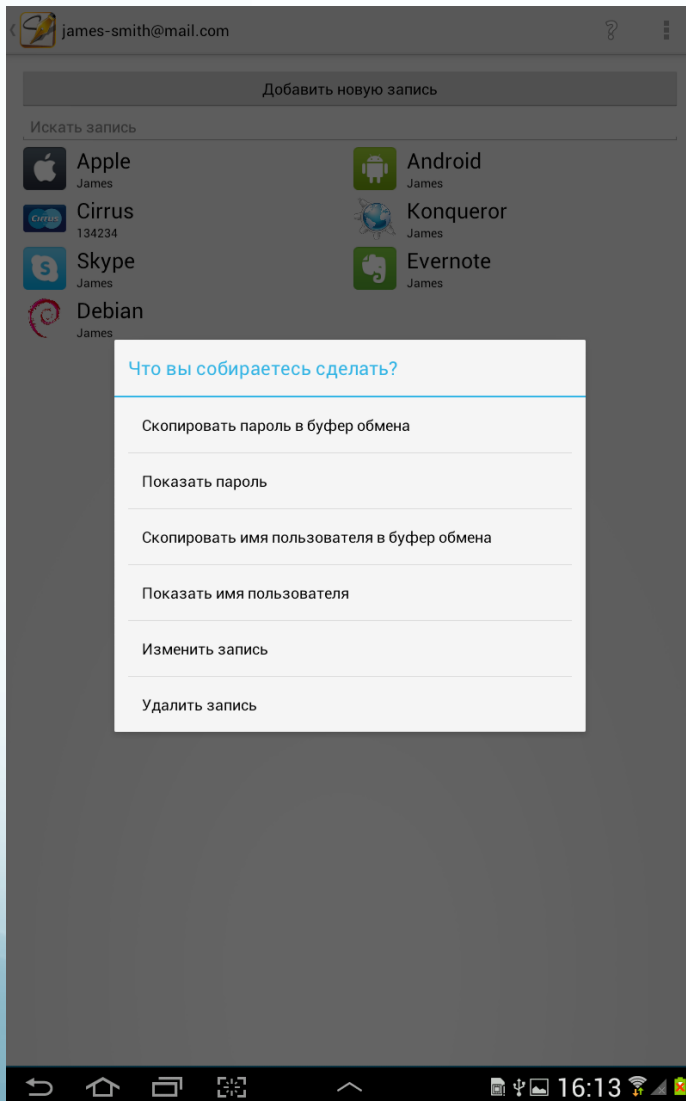
Внешний вид приложения



Оптимизировано для смартфонов и планшетов



Поддержка русского и английского языка



Регистрация вида подписи, скорости, давления на экран



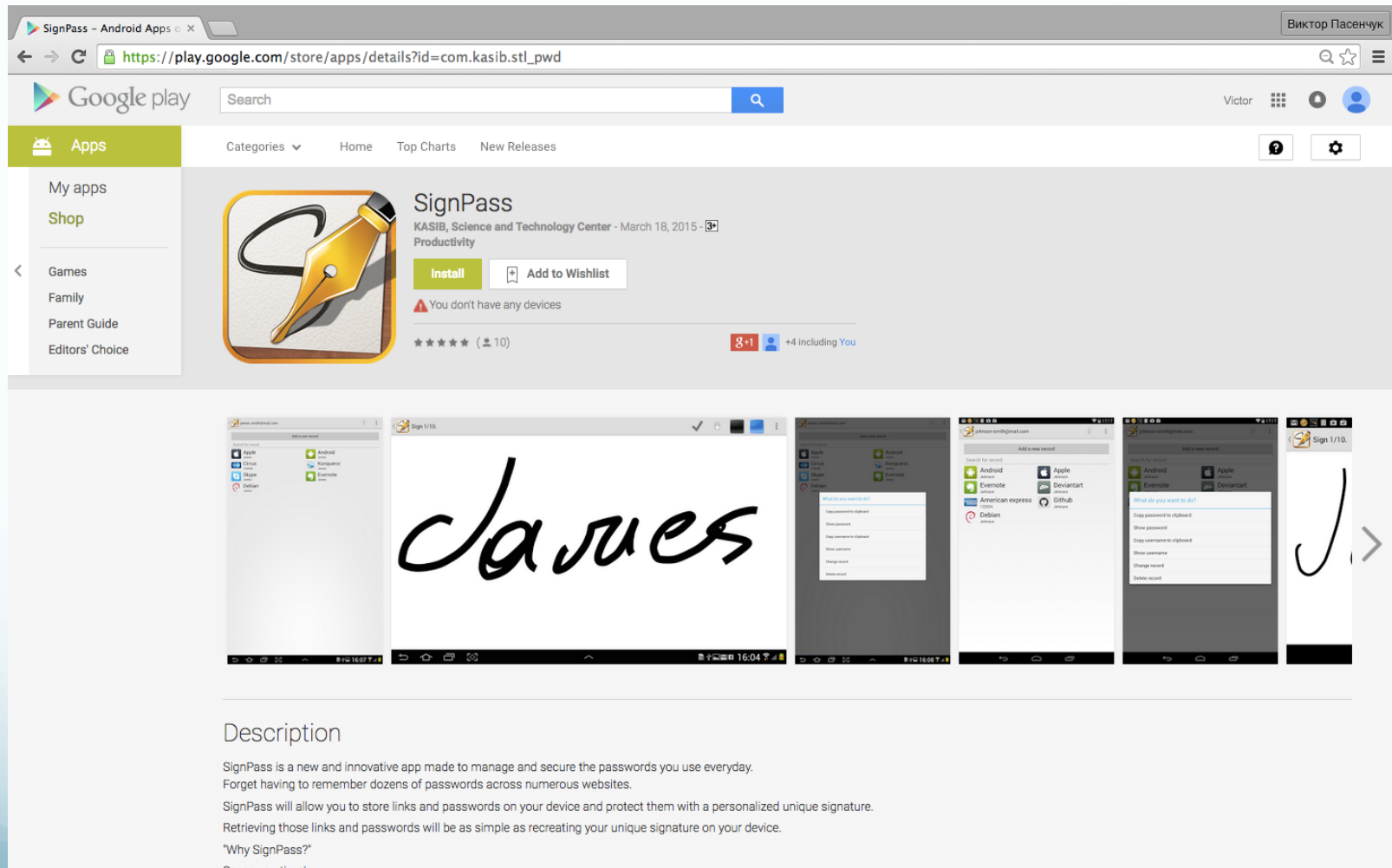
6. SignPass - итоги

- Приложение SignPass предназначено для хранения аутентификационных данных пользователей.
- Утеря подобной информации в большинстве случаев не может привести к большим убыткам, так как существует возможность восстановления этих данных с помощью мобильного телефона или электронной почты.
- Попадание аутентифицирующей информации к третьим лицам может повлечь существенный вред владельцу этих данных.
- Приложение ориентировано на минимизацию вероятности ошибок второго рода. При тестировании ошибки второго рода зафиксированы не были.
- Ошибки первого рода не являются исключительной ситуацией и возникают в случае неаккуратного ввода подписи.

7. Публикация SignPass в Google Play

- Категория: производительность (работа).
- Поддержка: Android 2.2 (API v8) и выше.
- Локализации: русская, английская.
- Распространение: бесплатно.
- Средняя оценка: 4.75
- Ссылка:
https://play.google.com/store/apps/details?id=com.kasib.stl_pwd

Страница приложения в Google Play



SignPass

KASIB, Science and Technology Center - March 18, 2015 - 3+

Productivity

Install Add to Wishlist

You don't have any devices

★★★★★ (10) 8+1 +4 including You

Description

SignPass is a new and innovative app made to manage and secure the passwords you use everyday. Forget having to remember dozens of passwords across numerous websites.

SignPass will allow you to store links and passwords on your device and protect them with a personalized unique signature. Retrieving those links and passwords will be as simple as recreating your unique signature on your device.

"Why SignPass?"

Saves you time!

Коммерциализация

- Монетизация приложения – отсутствует, приложение полностью бесплатное.
- Рабочие экраны (просмотр, создание, ввод, редактирование записей) не содержат баннеров и прочих раздражающих факторов, отвлекающих от основного функционала.
- Облачная платформа верификации по рукописной подписи SignToLogin, разработанная в НТЦ Касиб, допускает коммерческое использование. Информация: <https://signtologin.com/>

8.1 Инструменты аналитики:

Google Play

- Аналитика по числу установок/удалений
- Отзывы пользователей
- Распределение по различным критериям: версия приложения, версия ОС, используемые устройства, оператор связи и т.п.
- В некоторых случаях – отчёты об ошибках

Отзывы

Оценки и отзывы - SignPass

← → ↻ 🔒 https://play.google.com/apps/publish/?dev_acc=07710934089033125104#ReviewsPlace:p=com.kasib.stl_pwd 🔍 ☆ ☰

🤖 Все приложения

🎮 Игровые сервисы

📊 Отчеты

⚙️ Настройки

🔔 Оповещения

🗨️ Уведомления

SignPass
com.kasib.stl_pwd
ОПУБЛИКОВАНО 18 марта 2015 г. Удалить из Google Play

Статистика

Оценки и отзывы

Сбои и ANR

Советы по оптимизации

Cloud Test Lab

Файлы APK

Данные для Google Play

Возрастные ограничения

Цены и распространение

Контент для продажи

Службы и API

Опубликовать обновление

ОЦЕНКИ И ОТЗЫВЫ Экспорт CSV-файла

Число оценок
10

★★★★★
★★★★★
★★★★★
★★★★★
★★★★★

7
3
0
0
0

Средняя оценка

4,70

Количество отзывов: #
3

★★★★★
★★★★★
★★★★★
★★★★★
★★★★★

0
0
0
0
0

ОТЗЫВЫ

Фильтры ▾

Упорядочить По времени обновления ⌵

★★★★☆
Версия: 1.1
L70 (w5ds)

Eugene Kayuda, 16 нояб. 2014 г. в 1:29
Автоперевод (язык оригинала: Болгарский)
Реклама Показать оригинал
Вы ответили 20 июня 2015 г. в 2:43
Рекламы больше нет, приложение теперь полностью бесплатное.
Изменить

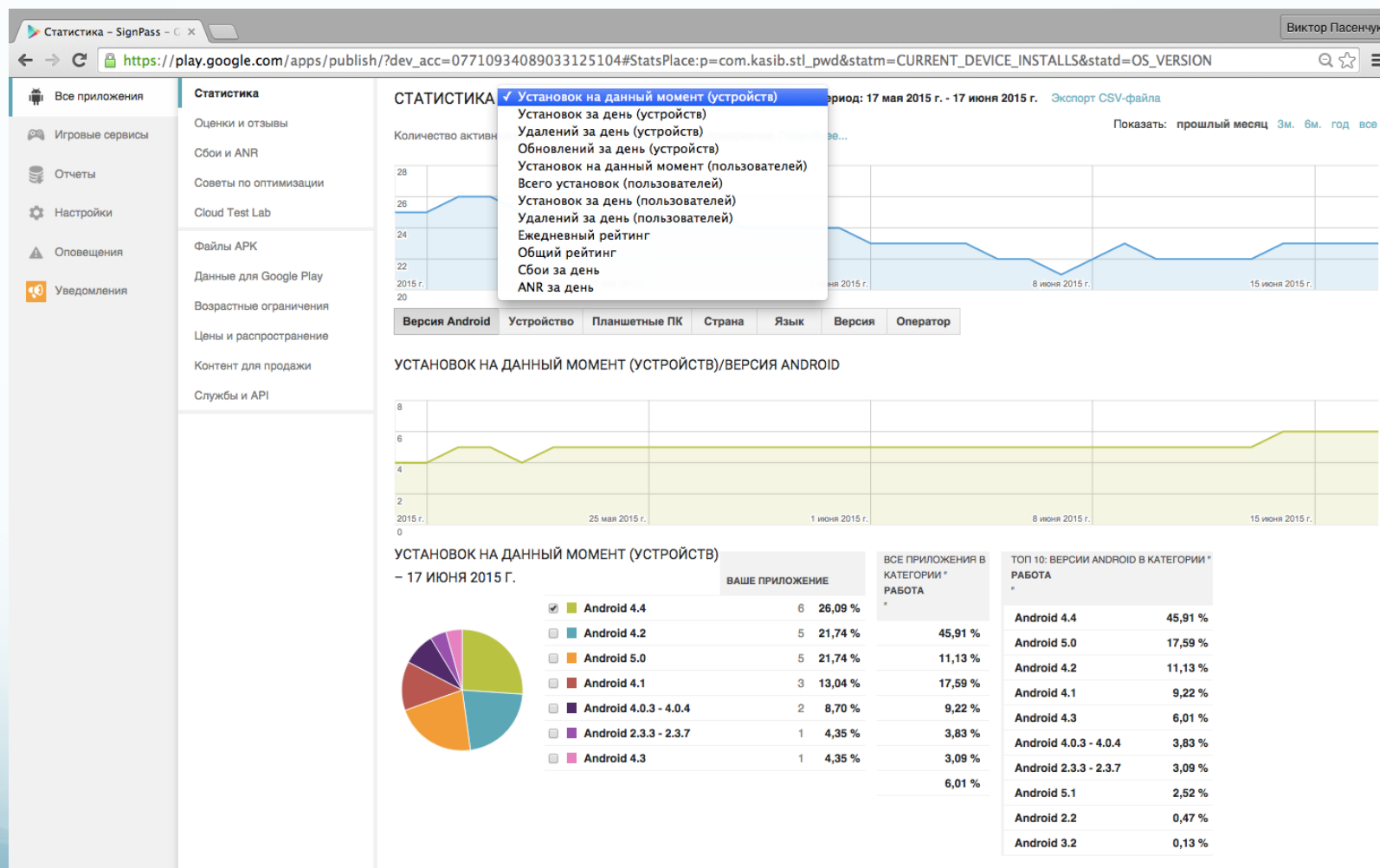
★★★★★
Версия: 1.0
Xperia C (C230S)

MrGremlin069, 13 окт. 2014 г. в 8:42
Хорошее приложение. Все функции работают стабильно.
Ответить

★★★★★
Версия: 1.0
HTC One X+ (enrc2b)

Пасенчук Виктор, 11 окт. 2014 г. в 22:32
Автоперевод (язык оригинала: Английский)
Ницца приложение. Классная идея использовать почерк войти. Скрыть оригинал
Отзыв на языке оригинала
Nice app. Cool idea to use handwriting to login.
Вы ответили 11 окт. 2014 г. в 22:48
Thanks for review.
Изменить

Выбор критериев



Распределение по версии ОС

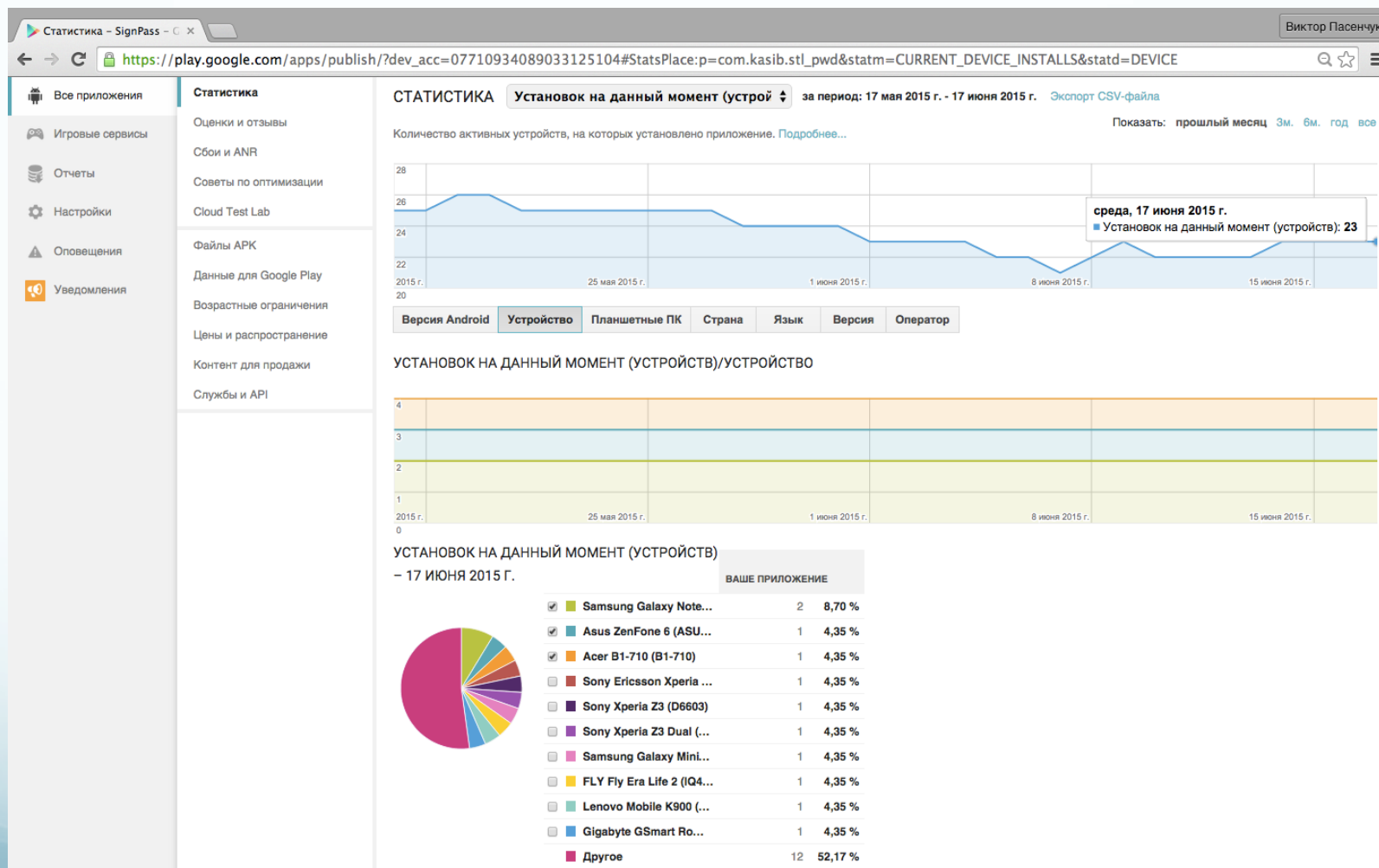
УСТАНОВОК НА ДАННЫЙ МОМЕНТ (УСТРОЙСТВ)
– 17 ИЮНЯ 2015 Г.

ВАШЕ ПРИЛОЖЕНИЕ



☒	Android 4.4	6	26,09 %
☒	Android 4.2	5	21,74 %
☒	Android 5.0	5	21,74 %
☐	Android 4.1	3	13,04 %
☐	Android 4.0.3 - 4.0.4	2	8,70 %
☐	Android 2.3.3 - 2.3.7	1	4,35 %
☐	Android 4.3	1	4,35 %

Распределение по устройствам



Распределение по устройствам

УСТАНОВОК НА ДАННЫЙ МОМЕНТ (УСТРОЙСТВ)

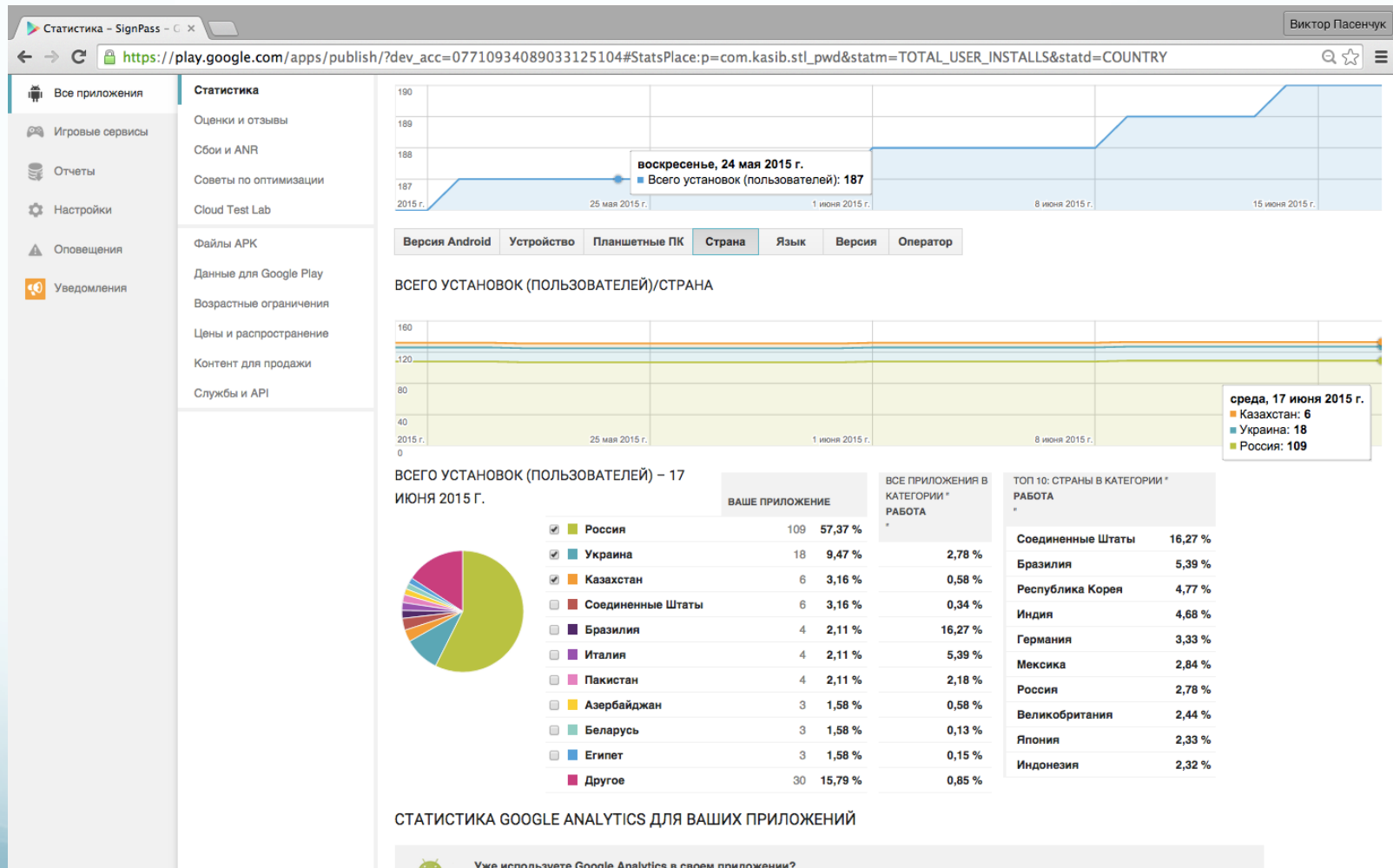
– 17 ИЮНЯ 2015 Г.

ВАШЕ ПРИЛОЖЕНИЕ



☒	 Samsung Galaxy Note...	2	8,70 %
☒	 Asus ZenFone 6 (ASU...	1	4,35 %
☒	 Acer B1-710 (B1-710)	1	4,35 %
☐	 Sony Ericsson Xperia ...	1	4,35 %
☐	 Sony Xperia Z3 (D6603)	1	4,35 %
☐	 Sony Xperia Z3 Dual (...	1	4,35 %
☐	 Samsung Galaxy Mini...	1	4,35 %
☐	 FLY Fly Era Life 2 (IQ4...	1	4,35 %
☐	 Lenovo Mobile K900 (...	1	4,35 %
☐	 Gigabyte GSmart Ro...	1	4,35 %
	 Другое	12	52,17 %

Распределение по странам



Распределение по странам

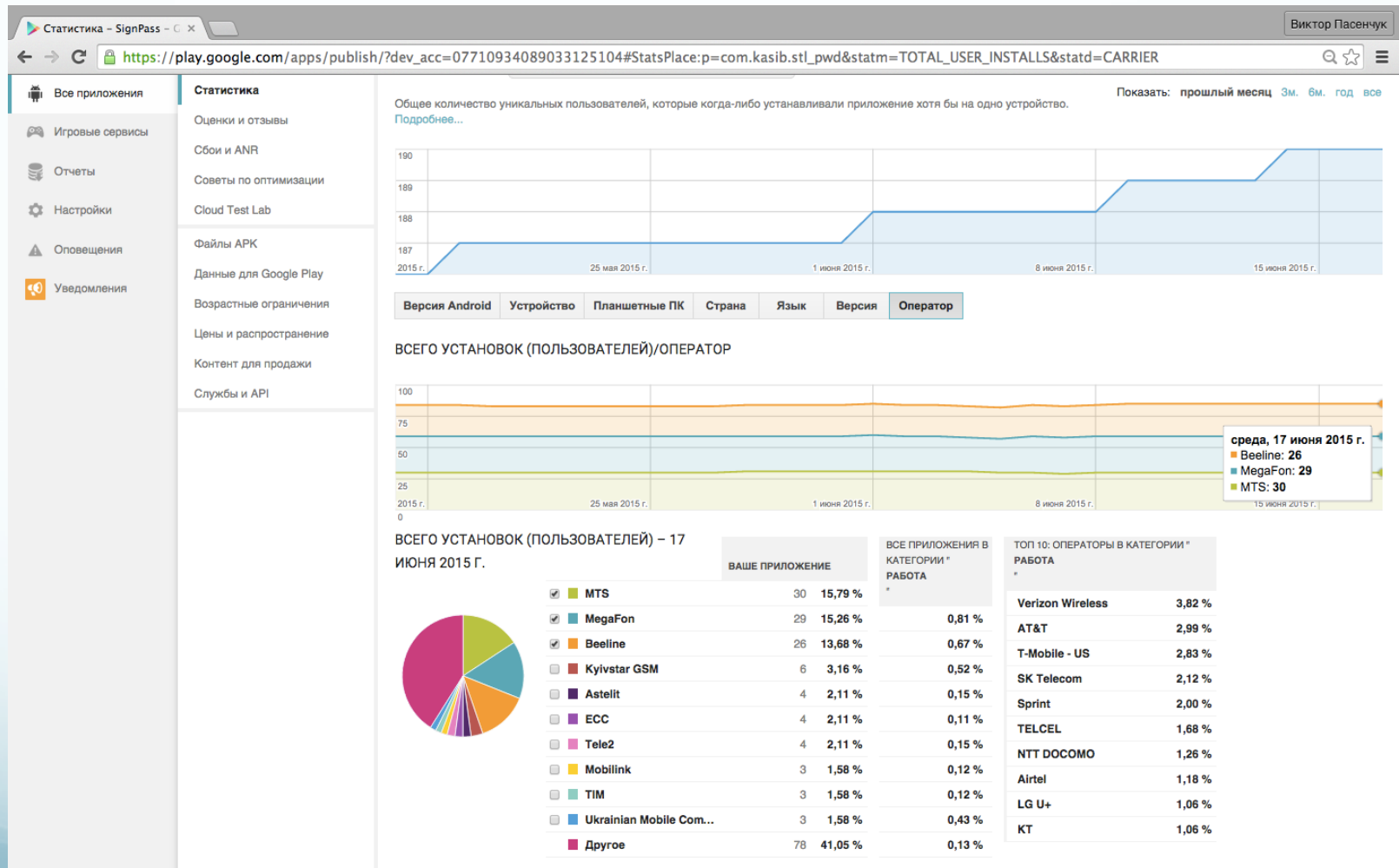
ВСЕГО УСТАНОВОК (ПОЛЬЗОВАТЕЛЕЙ) – 17
ИЮНЯ 2015 Г.



ВАШЕ ПРИЛОЖЕНИЕ

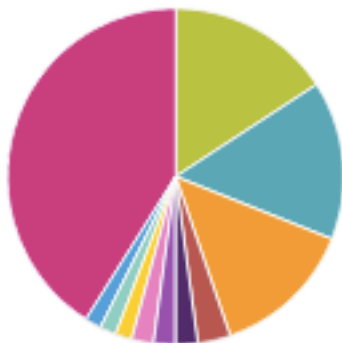
☒	Россия	109	57,37 %
☒	Украина	18	9,47 %
☒	Казахстан	6	3,16 %
☐	Соединенные Штаты	6	3,16 %
☐	Бразилия	4	2,11 %
☐	Италия	4	2,11 %
☐	Пакистан	4	2,11 %
☐	Азербайджан	3	1,58 %
☐	Беларусь	3	1,58 %
☐	Египет	3	1,58 %
☐	Другое	30	15,79 %

Распределение по операторам



Распределение по операторам

ВСЕГО УСТАНОВОК (ПОЛЬЗОВАТЕЛЕЙ) – 17
ИЮНЯ 2015 Г.



ВАШЕ ПРИЛОЖЕНИЕ

☒	MTS	30	15,79 %
☒	MegaFon	29	15,26 %
☒	Beeline	26	13,68 %
☐	Kyivstar GSM	6	3,16 %
☐	Astelit	4	2,11 %
☐	ECC	4	2,11 %
☐	Tele2	4	2,11 %
☐	Mobilink	3	1,58 %
☐	TIM	3	1,58 %
☐	Ukrainian Mobile Com...	3	1,58 %
	Другое	78	41,05 %

8.2 Инструменты аналитики: Crashlytics

- Crashlytics issues: получение подробных отчётов об ошибках: строка кода, вызвавшая ошибку, состояние устройства (ОЗУ, ПЗУ, заряд аккумулятора), количество ошибок.
- Crashlytics answers: динамика изменения количества активных пользователей, времени сессии, частот ошибок.
- Crashlytics beta: позволяет оперативно рассылать демонстрационные сборки тестерам.

Crashlytics issues

Fabric

Виктор Пасенчук

https://fabric.io/kasib/android/apps/com.kasib.stl_pwd/issues/55865ffaf505b5ccf035516b/sessions/55856c1302490001701be76ba9717c0a

Issue #1

JUN 21 2015 06:55 (UTC)

TOTAL CRASHES: 1

PasswordRecordFragment.java line 73
com.kasib.stl_pwd.ui.fragments.PasswordRecordFragment.initStLAdapter

DEVICE

- LG-D325
DEVICE
- Portrait
ORIENTATION
- On
PROXIMITY

OPERATING SYSTEM

- 4.4.2
ANDROID VERSION
- No
ROOTED
- Portrait
UI ORIENTATION

BATTERY 71%

RAM 23%

DISKSPACE 24%

Keys ☒ Logs

LEARN ABOUT CUSTOM KEYS

[More](#)

Fatal Exception: java.lang.RuntimeException
Unable to start activity ComponentInfo{com.kasib.stl_pwd/com.kasib.stl_pwd.ui.activities.AccountActivity}: java.lang.NullPointerException

[raw](#)

```
at android.app.ActivityThread.main(ActivityThread.java:5103)
at java.lang.reflect.Method.invokeNative(Method.java)
at java.lang.reflect.Method.invoke(Method.java:515)
at com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:790)
at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:606)
at dalvik.system.NativeStart.main(NativeStart.java)
Caused by: java.lang.NullPointerException
at com.kasib.stl_pwd.ui.fragments.PasswordRecordFragment.initStLAdapter(PasswordRecordFragment.java:73)
at com.kasib.stl_pwd.ui.base.StLListFragment.onViewCreated(StLListFragment.java:61)
at android.support.v4.app.FragmentManagerImpl.moveToState(FragmentManager.java:951)
```

Заключение

- В ходе выполнения данной работы была достигнута основная цель – создание альтернативного метода аутентификации для мобильных устройств. Предлагаемый метод использует в качестве аутентификатора рукописный пароль.
- Для реализации цели были выполнены все поставленные задачи
- Мобильное приложение доступно по ссылке https://play.google.com/store/apps/details?id=com.kasib.stl_pwd

Спасибо за внимание

