# Титул

Здравствуйте, уважаемый председатель и члены государственной экзаменационной комиссии.

Вашему вниманию представлена работа на тему «Разработка сервиса поведенческого анализа функционирования мобильных устройств на операционных системах андроид».

Работу выполнил студент Князев Константин.

Научный руководитель работы – Трубиенко Олег Владимирович

Научный консультант – Потерпеев Герман Юрьевич

# Актуальность проблемы

Актуальность данной работы обсуловлена ростом популярности мобильных устройств.

На слайде представлены графики, построенные по данным от компании StatCounter, собирающей статистику в разных it-отраслях по всему миру. На левом графике отражен рост популярности пк и мобильных устройств за последние 10 лет и видно, что с 17 года мобильные устройства стали составлять заметную конкуренцию персональным компьютерам, а по правому графику заметно, что за последний год тенденция роста популярности мобильных устройств сохраняется.

# Актуальность проблемы 2

Если рассмотреть популярные пользовательских операционных систем, то ОС андроид также с 17 года начала конкурировать с лидером ОС для ПК – Windows с сохранением этой тенденции.

Но не смотря на непрерывную работу вендоров над своими устройствами, безопасность мобильных устройств до сих оставляет желать лучшего.

# Цели и задачи

Таким образом целью данной работы является разработка программного решения для мониторинга функционирования мобильных устройств на ОС андроид.

Для достижения данной цели поставлена задача анализа современных мобильных ОС, выделение необходимых параметров мониторинга, анализ существующих средств поведенческого анализа мобильных устройств на ОС андроид и реализовать средство для мониторинга функционирования мобильного устройства.

# Угрозы информационной безопасности в компании

По данным лаборатории касперского наибольшую опасность для компании составляют действия пользователей, а именно действия сотрудников, инсайдеров и фишинговые атаки.

# Источники утечки информации в корпорации

Если обратиться к статистике InfoWatch, то можно сделать вывод, что действия сотрудников несут большую для компании угрозу нарушения ИБ, чем внешние щлоумышленники.

# Риски, которые несут инсайдеры

Обычно инсайдеры могут украсть конфиденциальную информацию для ее сбыта, обнародовать персональные данные или нарушить целостность или доступность информации.

# Сравнение средств поведенческого анализа мобильных устройств

На сегодняшний день уже существуют средства поведенческого анализа мобильных устройств на ОС андроид. Для их сравнения можно рассмотреть примеры, представленные в таблице.

TaintDroid – стало прорывным средством в сфере поведенческого анализа функционирования андроид и долгое время удерживало на себе внимание на многих конференциях.

CrowDroid – использует в своей системе машинное обучение, с помощью которого может предположить вредоносную активность в функционировании системы.

MsfVenom – популярное средство среди специалистов по информационной безопасности, входящее в набор штатных средств Kali Linux.

В таблице представлены достоинства и недостатки этих средств для решения контроля пользователей с целью предотвращения или предупреждения утечки информации в компании от их действий.

# Архитектура системы

На слайде представлена архитектура разработанной системы, которая состоит из мобильного приложения, которое комуницирует с сервером посредством HTTPS запросов.

Серверное приложение состоит из API, обрабатывающего запросы от мобильного приложения и клиентского приложения, слоя работы с данными и базой данных.

# Мобильное приложение

Мобильное приложение состоит из ряда модулей, каждый из которых собирает соответствующую ему информацию.

На левом рисунке представлен пользовательский интерфейс, намеренно упрощенный с целью предотвращения пользователем отключения какого-то из модулей. Интерфейс обладает лишь индикатором функционирования сервиса.

В связи с политикой функционирования приложений в системе андроид, фоновые сервисы должны создавать для пользователя постоянное уведомление от этого сервиса. Данный пример представлен на среднем рисунке.

На правом рисунке представлено сообщение об успешной отработке модуля приложения, подобным сообщением сопровождается отработка каждого модуля.

# Клиент-серверная часть системы

Клиент-серверная часть системы построена на .NET Core 3.1, это не последняя на текущий момент версия платформа разработки, но она наиболее популярная для хостингов.

C# – один из популярнейших и наиболее удобных языков программирования для разработки приложений.

IIS – набор сервисов для веб-служб от компании Microsoft.

Entity Framework Core – для работы с базой данных.

Sql Server – одна из популярнейших баз данных для хостингов.

А клиентское приложение построено на фреймворке React и библиотеке Redux

На текущий момент база данных состоит из одной таблице, схема которой представлена на левом рисунке. Этой таблицы достаточно для данного сервиса, так как она позволяет нормализовано хранить информацию, от всех модулей мобильного приложения.

Справа представлена панель для анализа собранных данных, для удобства ее использования панель обладает фильтрацией данных.

# Схема взаимодействия модулей

На данном слайде представлена общая схема работы сервиса. Цикл работы сервиса начинается с запуска фонового процесса на мобильном устройстве.

За исключением модуля уведомлений, все модули функционируют по общему принципу. Согласно политике разработки приложений для андроид, фоновые процессы могут быть перезапущены с интервалом не меньше минуты.

Уведомления могут быть удалены пользователем в период бездействия сервиса, для решения этой проблемы, модуль уведомлений подписывается на получение нового уведомления и при получении нового запускает цикл, схожий со всеми остальными модулями, представляющий собой агрегацию собранных данных, и их отправку на сервер.

На сервере, полученные данные проходят необходимую обработку и сохраняются в базу для последующего использования клиентским приложением.

Стоит отметить, что данное средство предполагает использование на корпоративных устройствах компании с получением от пользователя разрешения на обработку персональных данных, получение которого решается компанией в организационном порядке.

# Экономическое обоснование

С экономической точки зрения, исходя из разработки данного средства в течение полугода, на разработку ушло порядка 470 тысяч рублей и при условии продажи данного средства минимум за 25 тысяч рублей, окупаемость данного проекта составляет 21 месяц.

# Выводы

По итогу данной работы было реализовано средство, которое может выступать как в роли самостоятельного, так и дополнительного средства для системы информационной безопасности компании.

И все поставленные задачи были выполнены.

# Спасибо за внимание!