- Поддерживаемые ОС. Если вы планируете разрабатывать приложения для нескольких ОС (Windows, Android, iOS и т. д.), еще возникнет вопрос о технической поддержке.
- Особенности. Хоть инструменты дополненной реальности, имеющиеся на рынке, имеют одинаковые функции, но не все похожи. Внимательно сравните каждую платформу, убедитесь, в наличии необходимых вам функции. Например, платформы могут не поддерживать геолокацию.

3. Выводите приложение на рынок.

Здесь речь идет о продвижении и повышении узнаваемости приложения. Этот этап очень важен, поскольку в магазинах приложений лежат десятки тысяч невостребованных приложений. Это важно еще и потому, что пользователи должны знать, как пользоваться дополненной реальностью.

Шаг 1. Создайте демонстрационное видео: сделайте рекламные и обучающие видеоролики, демонстрирующие, как пользоваться AR.

Шаг 2. Разместите инструкции в приложении: добавьте к ним примеры или даже фотографии и видео в приложении.

Шаг 3. Дайте пользователям возможность поделиться AR-контентом: добавьте соцсети и другие подключаемые модули, чтобы покупатели с удовольствием репостили фотографии с AR-изображениями или видео, размещали посты и твиты с фирменным хэштегом. [4]

В данной работе мной были раскрыты основные моменты, на которые стоит обратить внимание при внедрении дополненной реальности в работу интернет-магазина.

Список используемых источников:

1. Выдающийся опыт AR в розничном секторе // Hackernoon. URL: https://hackernoon.com/outstanding-ar-experiences-in-the-retail-sector-2963f674bca2 (дата обращения: 23.01.2020).
2. Визуальные технологии в ритейле // RETAILER. URL: https://retailer.ru/vizualnye-tehnologii-v-ritejle/ (дата обращения: 25.01.2020).
3. Дополненная реальность в интернет-магазине. Как это работает и нужно ли ее внедрять? // Oborot.ru. URL: https://oborot.ru/articles/dopolnennaya-realnost-v-internet-magazine-kak-eto-rabotaet-i-nuzhno-li-ee-vnedryat-3-i125991.html (дата обращения: 25.01.2020).
4. Как технически внедрить дополненную реальность в работу интернет-магазина // Oborot.ru. URL: https://oborot.ru/articles/kak-tehnicheski-vnedrit-dopolnennuyu-realnost-v-rabotu-internet-magazina-i127455.html (дата обращения: 25.01.2020).

ОБЗОР ИСТОЧНИКОВ УЯЗВИМОСТЕЙ ПЛАТФОРМ GOOGLE ANDROID И APPLE И ПРИМЕНЯЕМЫХ МЕТОДОВ ИХ РЕШЕНИЯ.

И.А. Буткеев, студент группы З-17В70,
научный руководитель Чернышова Т.Ю., к.т.н., доцент
Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета
652055, Кемеровская обл., г. Юрга, ул. Ленинградская, 26
E-mail:ivanless@yandex.ru

Аннотация: Цель данной статьи – выявить, в ходе исследования, отличия уровней безопасности платформ iOS и Android. Сравнить методы и сопряженные с ними трудности в обеспечении полной, гарантированной защиты конфиденциальности пользовательских данных. В статье рассматриваются общие для проблемы платформ, сходства и различия природы уязвимостей и имеющихся методов устранения. Все названные вопросы предлагаются к рассмотрению безотносительно конкурентного положения правообладателей и производителей на рынке высокотехнологичных электронных устройств.

Abstract: The purpose of this article is to identify, in the course of the study, the differences between the security levels of the iOS and Android platforms. Compare the methods and the difficulties associated with them in ensuring complete, guaranteed protection of the confidentiality of user data. The article discusses the common problems of platforms, similarities and differences in the nature of vulnerabilities and available methods of elimination. All these issues are proposed for consideration regardless of the competitive position of copyright holders and manufacturers in the market of high-tech electronic devices.

Ключевые слова: Apple, iOS, Google, Android, безопасность, защита конфиденциальности, обновление безопасности, уязвимость, приложение, показатель сбоев.

Keyword: Apple, iOS, Google, Android, Security, Privacy protection, Security update, vulnerability, app, Crash rate.

Основные функции iOS и Android не отличаются. В устройствах под управлением iOS и Android есть общие для платформ функции: телефонный вызов по абонентскому номеру, обмен короткими сообщениями, просмотр веб-страниц, видеосвязь, навигация, голосовое управление и другие.

Основные различия между iOS и Android заключаются в следующем:

iOS - закрытая система, а Android - более открытая. В iOS у пользователей почти нет системных разрешений, но в Android пользователи могут легко настраивать параметры системы. Android основана на ядре Linux (монолитное ядро Debian). iOS основана на синтезе Darwin OS и FreeBSD (гибридное ядро).

Приложения Android выполняются изолировано от неиспользуемых ресурсов системы до тех пор, пока пользователь не предоставит самостоятельно доступ приложению. Такое разделение, в целом, повышает защищенность системы, но как итог – многие приложения запрашивают не всегда нужные им разрешения.

Безопасность устройств под управлением Android и iOS в большой мере зависит от своевременного обновления ПО. iOS имеет огромное преимущество из-за сильной фрагментации Android – экосистемы, включающей множество аппаратных платформ от различных производителей устройств. Apple выпускает обновления для всех устройств под управлением iOS одновременно. Так же все устройства Apple получают последнюю версию firmware. Но не следует забывать, что Apple так же является единственным производителем этих устройств. И, кстати говоря, iOS и Mac OS являясь полностью бесплатными для конечного пользователя, не могут быть использованы законно на любых устройствах, кроме устройств Apple. С устройствами под управлением Android все гораздо сложнее, так как множество различных производителей сначала должны получить от Google обновления безопасности для своих платформ, затем адаптировать их; получить одобрение Google и только после этого сделать их доступными для своих устройств по всему миру. Учитывая, что таких производителей более 500, а конфигураций и разновидностей устройств ещё больше, невозможно закрыть даже однотипные уязвимости одним патчем. К тому же производители отказываются от поддержки своих устройств через 18 – 24 месяца, продолжая выпускать только критические обновления безопасности. У Android есть еще одна немаловажная проблема – большая фрагментация по версиям firmware внутри экосистемы (рисунок 1).

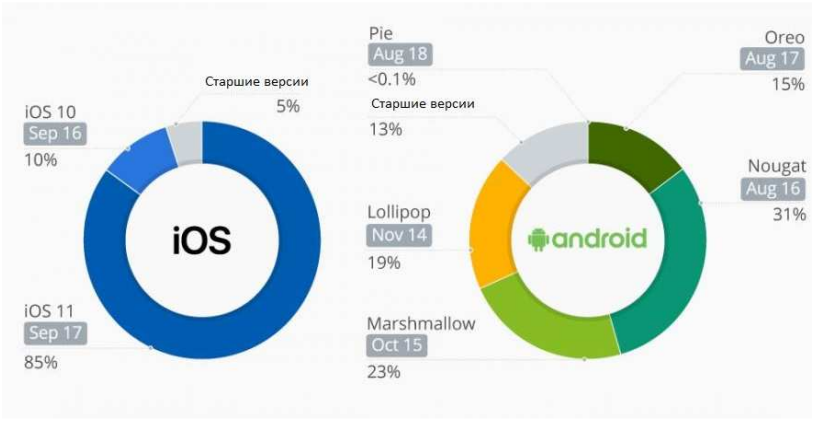

Рис. 1. «Диаграмма фрагментации экосистем Android и Apple по версиям продуктов.»

О том, какие устройства менее безопасны, также свидетельствует размер вознаграждений пентестерам за информацию об уязвимостях нулевого дня (т. е. ранее неизвестные) для iOS (1,5 миллиона долларов) и Android (200 000 долларов).

И iOS, и Android «уязвимы» для утечки данных через делегирование прав приложениям: приложение, будучи единожды установленным на устройство, получает полный список программ, ранее на этом же устройстве установленных. Следовательно, приложение-справочник получает информацию о том, что на устройстве установлено приложение онлайн-магазина, и передает издателю соответствующие сведения, которые могут быть использованы издателем любым возможным образом по его усмотрению.

В отчете Crittercism Mobile Experience Report от 2014 года, Android «KitKat» выделен как наиболее стабильный, в сравнении iOS 7.1. Отчет содержит и иные выводы, среди которых: высочайший уровень программных сбоев - 1,7% имеет Android 2.3 Gingerbread. Тогда как другие релизы Android - имеют коэффициент сбоев 0,7%. Среди них Jelly Bean. Ice Cream Sandwich, KitKat

Коэффициент отказов и сбоев iOS 7.1 составил 1,6%. Для iOS 7.0 - 2,1%. iOS 5 - 2,5%.

Релизы firmware Android и iOS для смартфонов более отказоуствойчивы, чем для планшетов.

В зависимости от категории приложения коэффициент сбоев так же очень сильно изменяется - игры (4,4% сбоев), а у приложений электронной коммерции самый низкий показатель сбоев - 0,4% рисунок 2.

Рис. 2. «Устойчивость к сбоям»

Помимо списка приложений, когда возникает задача защиты персональных данных пользователей, лидирующие позиции занимает iOS. До выхода в 2015 году Android Marshmallow, при первом запуске после установки требовалось предоставить все запрашиваемые разрешения. Это был своеобразный безальтернативный выбор из вариантов – предоставить приложению все разрешения или не использовать приложение. В Android M (Marshmallow) появилась возможность выдать необходимый минимум разрешений, нужных для запуска приложения и далее, при возникновении необходимости использовать весь функционал приложения, выдать дополнительные.

Список используемых источников:

1. 3DNews Исследование Crittercism: Android . [Электронный ресурс]. – Режим доступа: https://3dnews.ru/814838 (Дата обращения 29.01.2021).
2. It-brains Архитектура Apple iOS. [Электронный ресурс]. – Режим доступа:https://ru.it-brain.online/question/apple-ios-architecture/ (Дата обращения 29.01.2021).
3. Антивирусная Лаборатория Касперского. Превентивная защита «Что безопаснее Android или iOS?». [Электронный ресурс]. – Режим доступа:https://www.kaspersky.ru/resource-center/preemptive-safety/android-vs-ios (Дата обращения 27.01.2021).
4. RAZNOSOLIE Различия iOS и Android на техническом уровне. [Электронный ресурс]. – Режим доступа: http://raznosolie.ru/razlichiya-ios-i-android-na-texnicheskom-urovne/ (Дата обращения 29.01.2021).
5. ITIGIC Что лучше: Android 11 или iOS 14? . [Электронный ресурс]. – Режим доступа: https://itigic.com/ru/is-android-11-or-ios-14-better/ (Дата обращения 27.01.2021).