Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.42:621.395

Бородюк
Ольга Валерьевна

Методика анализа уязвимостей приложений для мобильных устройств

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

_____

Научный руководитель
Маликов Владимир Викторович
кандидат технических наук, доцент

_____

Минск 2019

ВВЕДЕНИЕ

В настоящее время в Республике Беларусь идет активная работа по развитию цифрового банкинга. Так была разработана специальная стратегия, основной целью которой является расширение к 2021 году взаимодействия банков, их клиентов, республиканских органов государственного управления и коммерческих организаций посредством электронных каналов коммуникаций.

Кроме того, одной из целей развития цифрового банкинга в Республике Беларусь является создание и поддержание необходимого уровня стабильности и безопасности функционирования цифровых технологий в финансовом секторе экономики, стандартизации безопасности.

Таким образом, необходимость проведения данного исследования обусловлена развитием рынка мобильных приложений, как внутри Республики Беларусь, так и за рубежом, а также появлением новых угроз безопасности, связанных с возможностью реализации злоумышленниками уязвимостей, результаты которых негативно влияют на обеспечение информационной безопасности персональных данных, финансовой информации пользователей, интеллектуальность собственности организаций и т.д.

Проведение периодической оценки защищенности мобильных приложений позволяет гарантировать высокий уровень их защищенности и минимизировать риски реализации угроз с последующими финансовыми и репутационными потерями для организации.

Целью данной работы является разработка методики анализа уязвимостей приложений для мобильных устройств.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016–2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в разработке методики анализа уязвимостей приложений для мобильных устройств.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

– Проанализировать существующие архитектуры мобильных приложений;

– Систематизировать основные уязвимости программного обеспечения и причины их возникновения;

– Определить модель нарушителя информационной безопасности и угрозы для мобильных приложений;

– Изучить основные подходы поиска уязвимостей и автоматизированные средства для упрощения данного процесса;

– Разработать и апробировать методику анализа уязвимостей мобильных приложений.

Апробация результатов диссертации

Материалы, вошедшие в диссертационную работу, докладывались и обсуждались на XIV Международной научно-практической конференции «Управление информационными ресурсами» (Минск, 2017 г.); на XVI Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, 2018 г.); на XVIII Межународно-технической конференции «Современные средства связи» (Минск, 2018 г.).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 3 работы, в том числе 3 тезиса докладов в сборнике материалов конференций.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения и библиографического списка. Общий объем диссертации 79 страниц, 46 наименований в библиографическом списке.

Во введении обоснована актуальность темы исследования.

В первой главе рассматриваются архитектуры современных мобильных приложений, современные угрозы информационной безопасности.

Далее на рисунке 1 приведена модель угроз информационной безопасности для мобильного приложения.

Рисунок 1 – Модель угроз информационной безопасности для мобильного приложения

Также в первой главе приведены статистические данные по уязвимостям популярным для мобильных приложений. Можно выделить следующий перечень уязвимостей:

– Обход архитектурных ограничений;
– Небезопасное хранение данных;
– Небезопасная передача данных;
– Небезопасная аутентификация;
– Слабая криптостойкость;
– Небезопасная авторизация;
– Контроль содержимого клиентских приложений;
– Модификация данных;
– Анализ исходного кода;
– Скрытый функционал.

В первой главе приведены причины возникновения уязвимостей в мобильных приложениях. Несмотря на то, что компании стремятся устранять уязвимости, ошибки в программном коде, допущенные при разработке и развертывании системы являются основными причинами возникновения угроз и реализации уязвимостей, что говорит о необходимости определения алгоритма оценки качества, который позволит предупреждать появление уязвимостей в приложениях для мобильных устройств еще на этапе проектирования

Во второй главе рассмотрены основные подходы к поиску уязвимостей в мобильных приложениях: статический и динамический анализ. Так применение статического анализа совместно с динамическим анализом приложений, позволяет комплексно подойти к оценке защищенности приложений для мобильных устройств и получить достоверные сведения об их состоянии.

Также во второй главе приведено краткое описание основных инструментов, которые на сегодняшний день используются для оценки защищенности мобильных приложений, и описан жизненный цикл безопасной разработки мобильного приложения, которые позволяет использовать наилучшие практики безопасного кодирования и выявлять уязвимости на всех этапах разработки (рисунок 2).

Рисунок 2 – Концепция жизненного цикла безопасной разработки

Третья глава посвящена разработке методики анализа уязвимостей мобильных приложений (рисунки 3 и 4), разработке алгоритма оценки качества приложений на этапе проектирования (рисунок 5), а также их апробации.

Разработанная методика базируется на методологии OWASP. Отличительной особенностью является углубленный анализ защищенности веб-ресурса, а также форма представления информации: разработанная методика выполнена в виде пошаговой инструкции. На рисунках 3 и 4 старые

блоки обозначены черным цветом, новые – красным, удаленные – красным пунктиром.

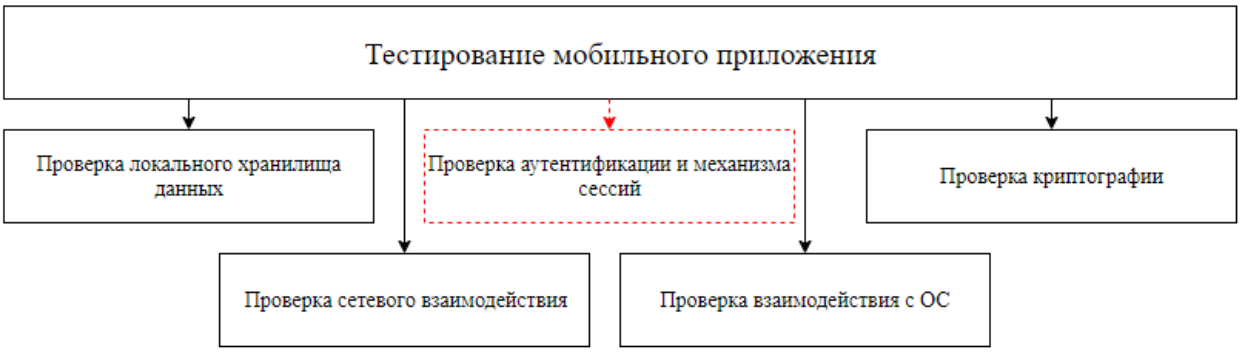

Рисунок 3 – Блок-схема разработанной методики тестирования (тестирование мобильного приложения)

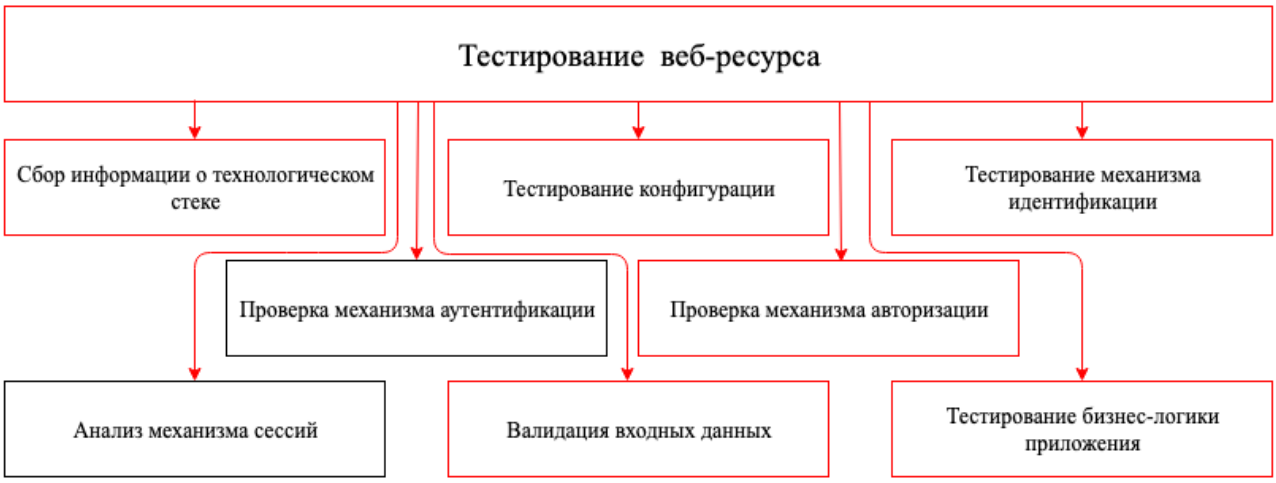

Рисунок 4 – Блок-схема разработанной методики тестирования (тестирование веб-ресурса)

В ходе разработки алгоритма оценки качества (рисунок 5) при проектировании мобильных приложений были выделены следующие критерии оценки защищенности:

– Соблюдение принципа уменьшения поверхности атаки;
– Соблюдение принципа наименьших достаточных привилегий;
– Соблюдение лучших практик для механизма аутентификации;
– Соблюдение лучших практик для авторизации;
– Выбор криптографических алгоритмов;
– Выбор сторонних сервисов;
– Валидация ввода.

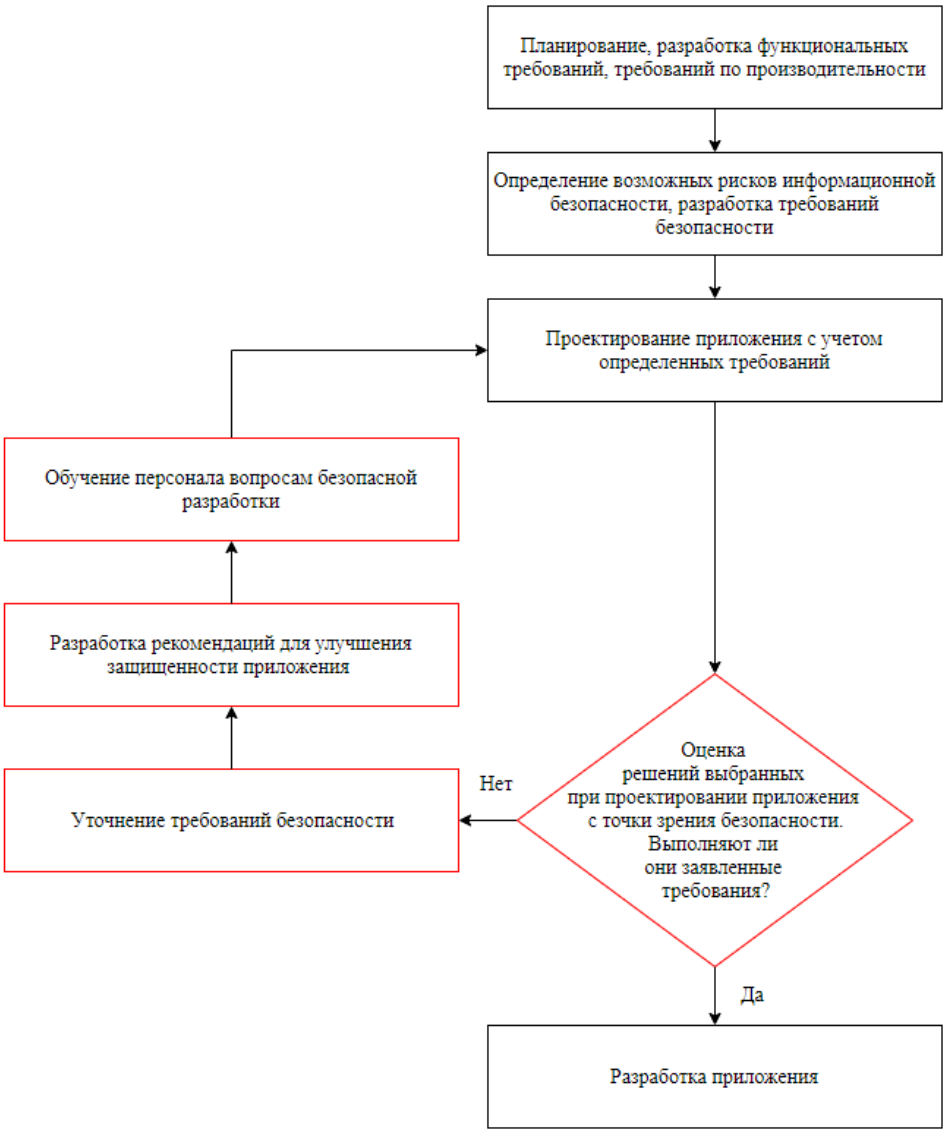

Рисунок 5 – Разработанный алгоритм обеспечения качества

При апробации разработанных методики и алгоритма в качестве типового объекта использовалось мобильное приложение «Android-InsecureBankv2». Результаты показали, что приложение имеет низкий уровень защищенности, поэтому в главе также были приведены рекомендации, которые можно применить к уже готовому приложению или находящемуся на стадии проектирования.

ЗАКЛЮЧЕНИЕ

В ходе проведения исследования было установлено, что для обеспечения высокого уровня защищенности мобильных приложений необходимо обеспечивать безопасность их программной части (исходного кода), конфигурации пакета приложения и сервера, а также повышать осведомленность и компетентность сетевого администратора.

В рамках данной работы были рассмотрены наиболее популярные архитектурные решения на рынке мобильных приложений, определены модель нарушителя и угрозы информационной безопасности. Также были рассмотрены десять наиболее распространенных уязвимостей, среди которых обход архитектурных ограничений, небезопасные хранение и передача данных, аутентификация и авторизация, слабая криптостойкость. Приведены статистические сведения о количестве, критичности и динамике уязвимостей для мобильных приложений. Определено, что в большинстве случаев уязвимости мобильных приложений обусловлены некорректно составленным разработчиками программным кодом, что связано с допускаемыми ошибками или неиспользованием приемов безопасного программирования.

Рассмотрены основные подходы поиска уязвимостей мобильных приложений – статический и динамический анализ. Проанализированы особенности каждого из этих подходов.

Рассмотрены наиболее популярные инструменты, а также особенности их применения.

На основе результатов выполненного анализа разработана методика анализа уязвимостей приложений для мобильных устройств. С применением этой методики обеспечивается систематизирование процесса поиска их уязвимостей, а также его автоматизация за счет рационального использования специализированных утилит.

Преимуществом разработанной методики является её простота, универсальность и гибкость, что позволяет проводить анализ защищенности мобильных приложений даже не специалисту в области информационной безопасности, а, например, разработчику или тестировщику программного обеспечения. Также данная методика позволяет при необходимости расширить или сократить список проверок в зависимости от конфигурационных и функциональных особенностей оцениваемого приложения.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

[1–А] Бородюк, О.В. Тестирование приложений для платежей с мобильных устройств на соответствие требованиям стандарта OWASP/ О.В. Бородюк, В.В. Маликов // Управление информационными ресурсами: материалы XIV Междунар. науч.-практ. конф., Минск, 20 дек. 2017 г. /Акад. упр. при Президенте Респ. Беларусь; под общ. ред. М. Г. Жилинского; редкол.: Д.В. Мазарчук (отв. ред.) [и др.]. – Минск : Академия управления при Президенте Республики Беларусь, 2017. – С. 159 – 160.

[2–А] Бородюк, О.В. Проблема делегирования ответственности на пользователя при использовании платежных приложений на мобильных устройствах / О.В. Бородюк // Технические средства защиты информации: тезисы докладов XVI Белорусско–российской НТК, Минск, 5 июня 2018 г. / БГУИР; редкол.: Т.В. Борботько [и др.]. – Минск, 2018. – С. 24.

[3–А] Бородюк, О.В. Обход биометрической аутентификации в мобильных приложениях / О.В. Бородюк, А. Ф. Жукевич // Современные средства связи: материалы XXIII Междунар. науч.-техн. конф., 18–19окт. 2018 года, Минск, Респ. Беларусь ; редкол. : А. О. Зеневич [и др.]. – Минск : Белорусская государственная академия связи , 2018. –189с.