



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Московский технологический университет»

МИРЭА

Институт кибернетики

Кафедра информационной безопасности

Дипломная работа

по теме:

Оценка влияния программного продукта
«Мобильный банк» на уровень защищенности
абонентского терминала.

Дипломник: Трунов М.А.

Группа: ККСО-01-11

Научный руководитель:

Лебедев С.Л.

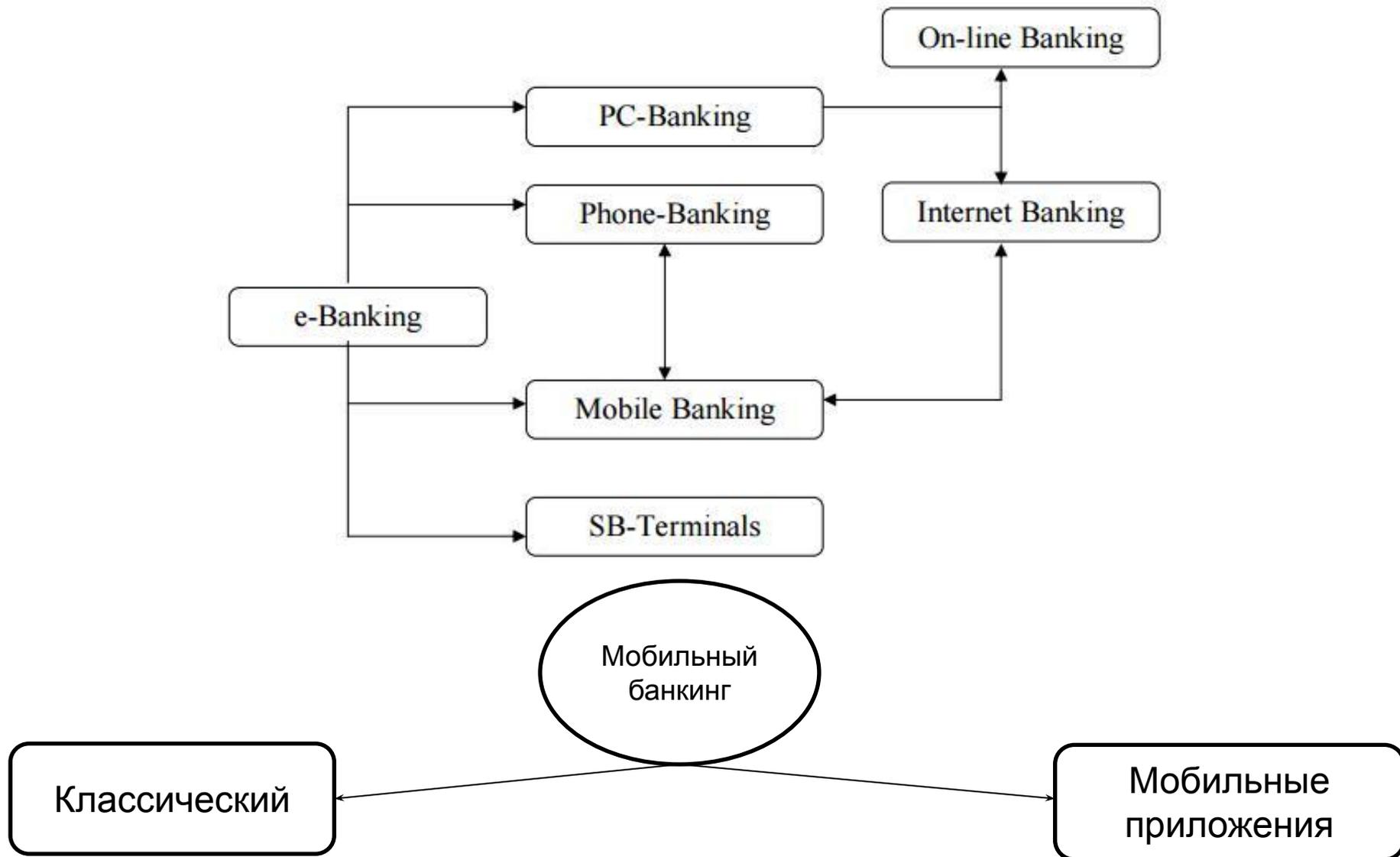
Москва, 2017

Количество атак на мобильные устройства за третий квартал 2016 года

Статистика «Лаборатории Касперского за третий квартал
2016 года»

- 1 520 931 вредоносных установочных пакетов;
- 30 167 установочных пакетов мобильных банковских троянцев;
- 37 150 установочных пакетов мобильных троянцев-вымогателей.

Классификация банковского обслуживания



Уязвимости мобильных приложений



Пример: **M2: Insecure Data Storage – Небезопасное хранение данных**

Содержит в себе 4 основные особенности:

- Hardcored and forgotten
- Некорректные права файлов
- Хранение данных приложения на SD-карте
- Логирование

Угрозы мобильным приложениям

- Root доступ
- Вирусы, вшитые в устройство на уровне системного ПО
- Троянские программы
 - Банковские трояны
 - Трояны, под видом обычного приложения
- RiskTool
- Мнение о том, что мобильные антивирусы защищают от всех угроз

Метод CVSS количественной оценки уязвимостей

CVSS Base Score	5
Impact Subscore	2.9
Exploitability Subscore	10
CVSS Temporal Score	4.1
CVSS Environmental Score	Not Defined
Modified Impact Subscore	0
Overall CVSS Score	4.1

[Show Equations](#)

CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C)

▼ Base Score Metrics

Exploitability Metrics	Impact Metrics
Access Vector (AV)*	Confidentiality Impact (C)*
Local (AV:L) Adjacent Network (AV:A) Network (AV:N)	None (C:N) Partial (C:P) Complete (C:C)
Access Complexity (AC)*	Integrity Impact (I)*
High (AC:H) Medium (AC:M) Low (AC:L)	None (I:N) Partial (I:P) Complete (I:C)
Authentication (Au)*	Availability Impact (A)*
Multiple (Au:M) Single (Au:S) None (Au:N)	None (A:N) Partial (A:P) Complete (A:C)

* - All base metrics are required to generate a base score.

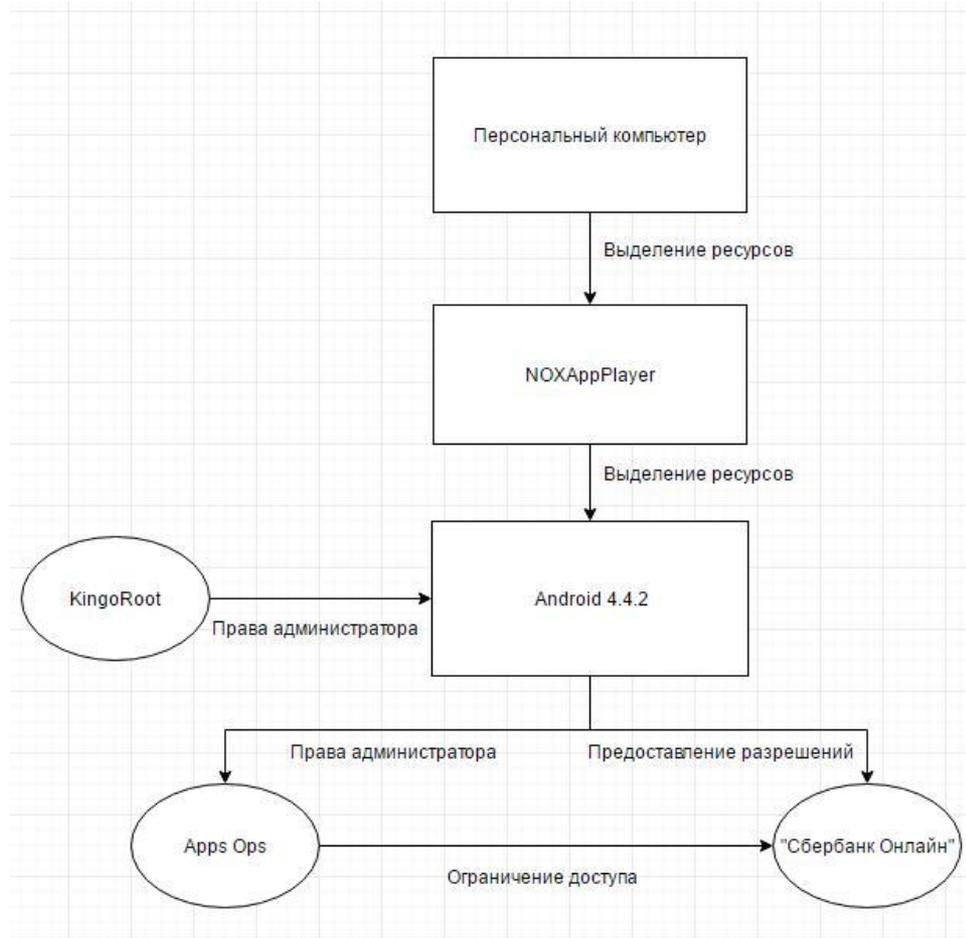
▼ Temporal Score Metrics

Exploitability (E)
Not Defined (E:ND) Unproven that exploit exists (E:U) Proof of concept code (E:POC) Functional exploit exists (E:F) High (E:H)
Remediation Level (RL)
Not Defined (RL:ND) Official fix (RL:OF) Temporary fix (RL:TF) Workaround (RL:W) Unavailable (RL:U)
Report Confidence (RC)
Not Defined (RC:ND) Unconfirmed (RC:UC) Uncorroborated (RC:UR) Confirmed (RC:C)

$$R = \sum_{j=1}^n P_r^j \cdot I^j \quad - \quad \text{Значение риска согласно стандарту ISO/IEC 27005}$$

P_r^j – вероятность реализации -й угрозы;
 I^j – значение ущерба от реализации j – й угрозы;
 n – число угроз.

Экспериментальный стенд



Потенциальные угрозы на основе анализа приложения

Уязвимость	Потенциальная угроза	Рекомендации по защите
Отсутствие защиты идентификатора при первом входе в приложение	Кража данных доступа	Использование голосового набора. Запрет на использование нестандартных средств ввода (клавиатур)
Перехват SMS сообщений с уникальными паролями для доступа в систему/подтверждения платежей	Утрата денежных средств/потеря доступа к учетной записи	Запрет установки приложения на устройство, в котором установлена SIM-карта, связанная с банковским счетом
Отсутствие ограничений на переводы	Утрата денежных средств	Введение в мобильное приложение ограничений на разовый/суточный перевод
Запрос слишком высоких прав доступа к приложению без острой необходимости	Утрата денежных средств, нарушение конфиденциальности информации	Отключение необязательных разрешений встроенными или сторонними решениями.

Некоторые рекомендации разработчикам ПО и пользователям

- Учитывать root-доступ при разработке приложений
 - Не хранить конфиденциальные данные на устройстве
 - Учитывать возможность пользователя копировать/вставлять данные, делать снимки экрана, резервировать данные, использовать сторонние клавиатуры
 - Не использовать отправку конфиденциальных данных через SMS/MMS
 - Использовать локальные инструменты по обнаружению изменений в коде
 - Запретить приложению писать информацию на SD-карту
-
- После покупки устройства переустанавливать ОС не средствами восстановления, а с официального сайта разработчика
 - Отключать «лишние» права установленным приложениям
 - Не использовать банковские приложения на одном устройстве с SIM-картой, на которую привязан счет.
 - Не использовать ПО, заменяющее стандартную клавиатуру пользователя

Выводы

В ходе данной дипломной работы были решены следующие задачи:

1. Рассмотрены угрозы и уязвимости мобильных устройств и мобильных приложений, их классификация и общий принцип работы.
2. Введена система количественной оценки риска и приведен пример ее использования.
3. Разработан экспериментальный стенд, представляющий из себя эмуляцию Android системы, рассмотрены запрашиваемые разрешения при установке мобильного приложения «Сбербанк Онлайн», на этом основании сделаны выводы и разработаны рекомендации для разработчиков и пользователей по защите мобильных приложений.