УДК 004.056.5:004.738.5(045)

ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В МОБІЛЬНИХ ПРИСТРОЯХ У СЕРЕДОВИЩІ OS ANDROID

О. О. Мелешко, доц.; ***О. С. Болотнікова***

Національний авіаційний університет

olena_b95@ukr.net

Основне завдання статті — дослідити можливі засоби захисту інформації з обмеженим доступом на мобільних пристроях у середовищі OS Android. Визначити які дані можна віднести до інформації з обмеженим доступом та можливі шляхи її витоку.

Ключові слова: OS Android, мобільні телефони, безпека інформації, засоби захисту інформації.

The basic task of this article is to investigate possible facilities of priv with a limit access on mobile devices in the environment of OS Android. Thus to define what data it is possible to attribute to information with a limit access, and possible ways of her source

Keywords: OS Android, mobile telephones, safety of information, facilities of priv.

ВСТУП

На сьогодні проблема захисту інформації з обмеженим доступом у мобільних телефонах стає дедалі актуальнішою, тому, що мобільний телефон є майже у кожного. Дана технологія є повноцінним обчислювальним пристроєм, що підтримує більшу частину функціоналу традиційних електронно-обчислювальної машини (ЕОМ) за значно менших розмірів, що дозволяє обробляти інформацію віддалено й оперативно, скоротивши на цьому час і зусилля, витрати часу на переміщення до комп'ютера, тому що мобільний пристрій знаходитися практично завжди при собі. Враховуючи той факт, що збережена інформація може містити в собі інформацію різного рівня (типу) конфіденційності, то втрата її може нести значні збитки.

Об'єктами захисту є інформація, що міститься та обробляється на мобільному телефоні, права власника цієї інформації та власника мобільного пристрою, права користувача має бути захищені.

Доступ до інформації, яка зберігається, обробляється і передається в мобільному пристрої, здійснюється лише згідно з дозволу власника інформації чи уповноваженою ним особою.

Без дозволу власника доступ до інформації, яка зберігається, здійснюється лише у випадках, передбачених чинним законодавством.

Постановка проблеми

Найпоширенішою операційною системою для смартфонів на сьогодні є Android. Ця платформа швидко розповсюджується через зручний інтерфейс, можливість налаштування системи, оскільки це зручно певному користувачеві.

Android — це портативна (мережева) операційна система для комунікаторів, планшетних комп'ютерів, електронних книжок, цифрових програвачів, наручних годинників, нетбуків і смартбуків, заснована на ядрі Linux. Це порівняно «молода» операційна система, використовувана на широкому спектрі мобільних пристроїв.

Завдяки своєї багатофункціональності, мобільні пристрої з операційною системою Android, можна віднести до ЕОМ, тому їм також притаманні слабкі місця з точки зору безпеки інформації, такі як [1, 2, 3]:

1. Можливість витоку інформації технічними каналами.
2. Можливість візуального зчитування інформації з дисплея пристрою.
3. Наявність вбудованої пам'яті на пристрої, або ж додаткової (флеш накопичувача).
4. Можлива наявність вразливостей в програмному та апаратному забезпеченні.

Особливостями ж самих мобільних пристроїв, що визначають для них загрози безпеки інформації, є:

1. Нестаціонарність (можливість непомітного винесення і повернення пристрою в контрольовану зону).
2. Компактні розміри.
3. Наявність дротових і бездротових інтерфейсів, за допомогою яких можна підключитися до даного пристрою.
4. Можливість використання пристрою як модем для підключення до мереж зв'язку загального користувача.
5. Можливість використання в якості знімного носія інформації (альтернатива флеш-накопичувача).

Розглянемо типові дані, що зберігаються на смартфоні, які можуть бути корисні для зловмисника і тому потребують захисту.

- Дані про облікові записи.

У випадку якщо ви налаштували синхронізацію з Facebook, Dropbox, Twitter, логіни і паролі

для цих систем зберігаються у відкритому вигляді в папці профілю телефону /data/system/accounts.db.

- **Jabber**-клієнт

Skype, Icq, Jabber — усе це не притаманне сучасним мобільним пристроям, внаслідок чого і листування цієї конкретної людини, і його співрозмовника, можуть бути під загрозою.

- Історія СМС-листування і телефонна книга.
- Дані Web-браузера.

У браузері можуть зберігатися дані для авторизації на сторонніх веб-серверах. У випадку якщо синхронізується мобільний браузер (Google Chrome, Firefox, Maxton і т. д.) з настільною версією браузера, слід врахувати, що з вашого смартфона (планшета) можна отримати доступ до всіх ваших паролів.

- Карта пам'яті.

Як правило, на карті зберігають фото- і відеозйомку.

- Документи, замітки.

Як було сказано раніше, на даний момент мобільні телефони можуть стати місцем зберігання, редагування якихось документів, так само як і різні замітки і події в календарі. Місткість сучасних пристроїв настільки велика, що вони могли замінити usb-накопичувачі, а документи і файли на них цілком здатні зацікавити зловмисників. Часто в смартфонах звичайні користувачі зберігають у замітках чи інших текстових редакторах, паролі, електронні адреси тощо.

Аналіз досліджень і публікацій

Для вирішення завдання захисту даної інформації залучають засоби безпеки, як вбудовані в систему, так і програмне забезпечення, що розроблено стороннім розробниками.

Вбудовані засоби захисту інформації

Вбудовані засоби захисту інформації, розглянемо на прикладі телефону на базі якого знаходиться операційна система Android

1. Блокування екрану смартфону

Розблокування екрану можливо при (див. рисунок):

1) Дотик до екрана мобільного телефону (Слайдер)

Для розблокування приладу, користувач повинен провести пальцем по екрану монітора, що й призводить до розблокування приладу. Використання цього способу не забезпечує збереження вашої інформації, через те що захист взагалі відсутній.

2) Розпізнавання обличчя (низький рівень безпеки)

Цей спосіб забезпечує низький рівень безпеки, оскільки людина з схожим типом обличчя, може розблокувати даний пристрій. Якщо ж користувач має намір використати саме цей тип блокування, то треба знайти місце з гарним освітленням й утримувати пристрій на рівні очей упродовж хвилини. Тоді фронтальна камера зафіксує контури вашого обличчя (ідентифікаційні дані), що будуть використані для ідентифікації особистості. Ці дані зберігатимуться у закритому доступі.

3) Блокування малюнком (середній рівень безпеки)

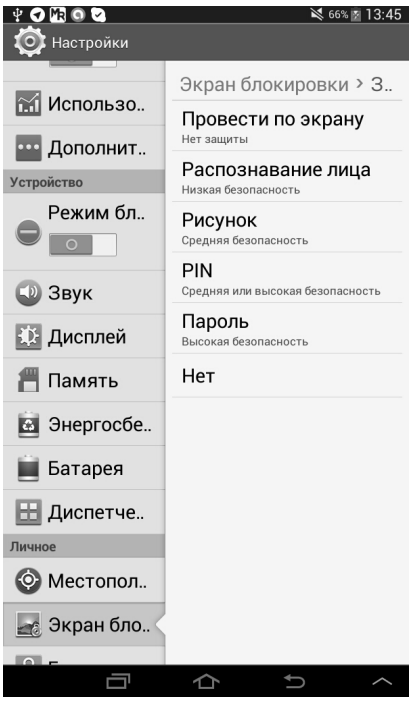
Блокування малюнком вважається системою середнього рівня захисту. Для його застосування користувач повинен з'єднати у будь-якому порядку не менше ніж 4 точки, тим самим створюючи свій унікальний ключ.

4) Введення PIN (середній чи високий рівень безпеки)

PIN – певна послідовність цифр, мінімальна довжина якого 4 символи. Чим більша кількість цифр, тим вище рівень захисту системи.

5) Введення паролю (високий рівень безпеки)

Введення паролю має найбільш високий рівень безпеки, оскільки в його склад входить не тільки цифри, а й букви.



Вбудовані засоби захисту інформації

2. Шифрування пам'яті телефону

Дана функція доступна не для всіх смартфонів, лише для пристроїв, що використовують OS Android 4.0 й вище.

Використати шифрування можливо лише у тому випадку, якщо у користувача встановлено блокування екрану за допомогою паролю.

За допомогою шифрування користувач може зберегти дані, що знаходяться в пам'яті телефону.

У користувача є можливість зашифрувати:

1. Обліковий запис.
2. Параметри.
3. Завантажені програми та їх дані.
4. Мультимедійні та інші файли.

Після шифрування пристрою, за кожного його включення для розшифрування вимагатиме PIN-код або пароль.

Необхідно врахувати, що програма при цьому не шифрує SD-карту.

Шифрування може зайняти до однієї години, це залежить від об'єму пам'яті на смартфоні.

У разі якщо користувач забув пароль, єдиним варіантом розблокування пристрою, це сброси до заводських налаштувань. При цьому всі дані, що зберігались на пристрої будуть втрачені.

Недоліки шифрування:

1. Дана послуга доступна в OS Android 4.0 й вище.

2. Доступно не на всіх моделях смартфонів. Найчастіше ця функція зустрічається в телефонах від Samsung, HTC, Philips.

3. Користувачу необхідно постійно вводити пароль, (6–10 символів) навіть якщо потрібно просто подзвонити.

4. Якщо користувач має бажання зняті захист, то зробити це можливо лише при повному перезавантаженні телефона. Відновив його до заводських налаштувань.

3. Шифрування зовнішньої SD-карти

Дана функція входить в стандартний набір пакету Android 4.1.1 й вищих версіях. Вона забезпечує надійний захист даних на зовнішній SD-карті. Тут можуть зберігатись лише фотографії, текстові файли з інформацією комерційного та особистого характеру.

Дозволяє зашифрувати файл на SD-карті, не змінюючи її назви, файлової структури із збереженням попереднього перегляду графічних файлів (іконок).

Файли, що зашифровані на даному пристрої, можна використовувати лише на ньому. При сбросі налаштувань до заводських, ключ для розшифрування буде видалений.

Користувач не зможе користуватись зашифрованим файлом на карті пам'яті SD, але незашифровані файли будуть доступні й надалі.

Функція потребує установки завдовжки не менше 6 символів, що має не менш ніж 1 цифра. При зміні пароля слідом йде автоматичне оновлення шифру.

Програмне забезпечення, що розроблено стороннім розробниками

(Додаткове програмне забезпечення)

Нині, існує багато програм, що прагнуть забезпечити безпеку мобільних телефонів, такі як:

- Антивіруси.
- Введення паролю чи PIN.
- Блокування малюнком.

Варіанти з введенням паролю чи блокуванням малюнком, майже нічим не відрізняється від вбудованих засобів блокування.

Різниця лише у тому, що розробники можуть надати можливість надати більш яскравіший інтерфейс, чи можливість заблокувати не весь смартфон, а лише його частину, певні папки, що потребують захисту.

Антивірусні програми

Ураховуючи, той фактор, що кількість Android пристроїв збільшується з кожним роком на мільйони одиниць, дуже часто з'являються новини про виявлення «троянів» і шкідливих програм, які заражають смартфони на Android.

Зазвичай зараження відбувається у процесі скачування програм із сумнівних джерел [1]. Тому стали розроблятися антивірусні програми, які працюють на платформі Android. Багато таких антивірусів додатково мають функції відстеження загубленого або вкраденого смартфона. Особливо необхідний антивірус для рутованих (Root-права) смартфонів.

Скачати антивірус для Android-смартфона можна в Android-маркеті. Там є як платні так і безкоштовні антивірусні програми. Найвідоміша безкоштовна антивірусна програма це — «Avast! Mobile Security». Багато антивірусних програм мають два режими роботи: платний (усі функції працюють) і безкоштовний (обмежений).

Висновок

Отже, розглянуті варіанти захисту інформації на смартфонах з платформою Android, можна зробити висновок — дана операційна система має як власні, внутрішні засоби захисту, так само може й підтримувати додаткові засоби захисту, розробленими іншими розробниками.

Вбудовані внутрішні засоби захисту є досить зручним інструментам захисту даних на мобільних телефонах. Враховуючи тип блокування, виділяють різні види безпеки. Вони досить ефективні, але від зовнішніх атак, тобто якщо хтось прагне зайти на мобільний телефон та подивитись якісь певні дані, то зловмисник зустрічає перешкоду, у вигляді: паролю, малюнка, розпізнавання обличчя чи PIN. Але від внутрішніх атак, вірусів дані засоби безпорадні. Водночас, як додаткове програмне забезпечення, може забезпечити, як безпеку від внутрішніх, так і від зовнішніх атак.

ЛІТЕРАТУРА

1. *Михайлов Д. М.* Защита мобильных телефонов от атак / Д. М. Михайлов, И. Ю. Жуков, А. М. М. Ивашко. — М. : Фойлис, 2011. —192 с.

2. *Якушин П.* Безопасность мобильного предприятия / П. Якушин // Открытые системы. — 2013. — № 1 (187). — С. 22–27.

3. *Панасенко А.* Влияние мобильных устройств на безопасность информации / А. Панасенко. — [Електронный ресурс]. — Режим доступу: http://www. anti-malware.ru/node/12301, 2013.

4. *Гилмор Дж.* Безопасность мобильных устройств для «Чайников» / Дж. Гилмор, П. Бирдмор. — М. : John Wiley & Sons Ltd, Chichester, West Sussex, England (Англия), 2013. — 54 с.

5. *Ванг Й.* Проблемы безопасности смартфонов / Й. Ванг, К. Стрефф, С. Раман //Открытые системы. СУБД. — М. : Изд-во «Открытые системы», 2013. — 27–31 с.

Стаття надійшла до редакції 23.11.2015