УДК 004.056:[004.451+004.382]

Манжай І.А.
викладач кафедри фінансів, обліку і аудиту Харківського економіко-правового університету

Проблеми захисту інформації на мобільних комп'ютерних пристроях з операційними системами Android та Apple iOS

Анотація. У статті розглянуто проблемні питання, які виникають під час захисту інформації на мобільних пристроях. Наведено визначення мобільних пристроїв та проведена їх класифікація, а також зазначені найбільш поширені операційні системи для мобільних пристроїв. Проаналізовано окремі поширені загрози для мобільних пристроїв. Запропоновані рекомендації щодо захисту мобільних пристроїв від несанкціонованого доступу.

Ключові слова: мобільні комп'ютерні пристрої, мобільні операційні системи, система захисту інформації, Android, Apple iOS.

Аннотация. В статье рассмотрены проблемные вопросы, возникающие во время защиты информации на мобильных устройствах. Дано определение мобильных устройств и проведена их классификация, а также указаны наиболее распространенные операционные системы для мобильных устройств. Проанализированы отдельные распространенные угрозы для мобильных устройств. Предложены рекомендации по защите мобильных устройств от несанкционированного доступа.

Ключевые слова: мобильные компьютерные устройства, мобильные операционные системы, система защиты информации, Android, Apple iOS.

Summary. Problem questions which arise up during information security on mobile devices are considered in the article. The definition of mobile devices and their classification, and identifies the most common operating system used for mobile devices. Some common threats to mobile devices are analyzed. Recommendations for the protection of mobile devices against unauthorized access are proposed.

Keywords: mobile computer devices, mobile operating systems, information security system, Android, Apple iOS.

Постановка проблеми. Інформація на сьогоднішній день на

ринку є товаром, ціна якого може перевищувати мільйони і навіть мільярди доларів. Захист її від зміни, знищення та крадіжки з кожним роком стає все більш складним завданням. Поява на ринку мобільних комп'ютерних технологій не лише спричинила витиснення звичайних персональних комп'ютерів з різних сфер діяльності соціуму, але й призвела до збільшення кількості та появи нових видів кіберзлочинів. Такі злочини часто пов'язані з викраденням персональних даних користувача. Тому перед компаніями-виробниками та користувачами їх продукції на теперішній час стоїть завдання запровадження ефективного механізму захисту персональних даних, які містяться на мобільних комп'ютерних пристроях.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми. Питання захисту інформації, яка зберігається на мобільних пристроях, досліджували Дж. Вайн, А. Голощапов, А. Кейс, С. Коматинэни, О. Манжай, Х. Махт, В. Носов, Г. Річард, Р. Роджерс, Дж. Сільв, И. Сколотнев, Н. Федотов, Д. Фелкер, Г. Шавловський та багато інших вчених.

Метою даної статті є аналіз основних проблем, які виникають під час захисту інформації, що міститься в мобільних комп'ютерних пристроях, та знаходження шляхів їх подолання.

Виклад основного матеріалу дослідження. Мобільний комп'ютерний пристрій – персональний комп'ютер, який може бути зручно транспортований одною людиною і здатний бути швидко увімкнений у робочий стан, найчастіше з автономним живленням, з опціональною можливістю бути підключеним до мережі електроживлення [1].

Мобільні комп'ютери включають кілька класів комп'ютерів, перелік яких розширюється з розвитком інформаційної техніки. До них відносять: ноутбук або лептоп, нетбук, планшети, трансформери та смартфони із вбудованими сучасними мобільними операційними системами: Symbian OS, яка створена компанією Symbian – спільним підприємством фірм Motorola, Ericsson, Nokia і Psion; BlackBerry OS, що випускаються компанією Research In Motion Limited (RIM), Windows Mobile та Windows Phone, що розроблені компанією Microsoft; Linux, Android, що розроблені компанією Open Handset Alliance (OHA), Mac OS X та Apple iOS, власниками яких є компанія Apple. Наведені мобільні комп'ютерні пристрої є багатофункціональними та виконують

функції персональних комп'ютерів. Кількість інформації, персональних даних користувача, що міститься в них, постійно збільшується з розширенням їх можливостей та становить великий інтерес для правопорушників.

На сьогоднішній день виділяють наступні загрози безпеці мобільних комп'ютерних пристроїв [2]:

1. *Викрадення або втрата мобільних пристроїв*. Небезпека цієї загрози полягає у тому, що зловмисник може отримати вільний доступ до мобільного пристрою, а відповідно і до персональних даних, одержавши наступну інформацію, яка збережена на цьому пристрої:

- паролі та інформація про обліковий запис електронної пошти;
- електронне листування;
- облікові дані в соціальних мережах, таких як Facebook, Google, В контакті, Одноклассники або Twitter;
- паролі, що збережені в браузері;
- інформація про кредитні операції та картки;
- паролі, збережені в таких додатках як Amazon і Google Wallet або в хмарному сервісі iCloud;
- номери телефонів контактів;
- відомості про захищені мережі Wi-Fi;
- фотографії і відео тощо.

2. *Ненавмисне розкриття даних.* На сьогоднішній день розробники надають користувачам різноманітну кількість додатків для розширення можливостей мобільних комп'ютерних пристроїв. Загроза полягає в тому, що користувач при встановлені додатків на пристрій дозволяє їм доступ до певних персональних даних. Маються на увазі, передусім, контакти та списки вхідних та вихідних дзвінків, фото- та відеофайли, інформація про Wi-Fi-мережу, історія використання пристроїв та додатків, мікрофон, ідентифікаційні дані, місцезнаходження. При цьому власник пристрою у більшості випадків не замислюється, що використовувані ним додатки можуть передавати особисту інформацію третій стороні, наприклад, дані про місцезнаходження користувача, його присутність або відсутність у певних місцях тощо.

Група авторів The Wall Street Journal свого часу провела журналістське розслідування, під час якого було виявлено, що деякі програми-додатки, розроблені для мобільних операційних

систем iOS і Android передають особисті дані користувача третім особам і рекламодавцям. У список програм-додатків, що перевірялися авторами, увійшла відома на iPhone гра Angry Birds. Під час дослідження виявилось, що саме ця гра передавала виробнику програмного забезпечення і його партнерам не тільки ім'я користувача та пароль до iTunes, але й місце розташування та контакти [3].

Авторами були зроблені наступні висновки:

- 56 % додатків передають унікальний номер апарата іншим компаніям (рекламним мережам) без будь-якого повідомлення або дозволу користувача;

- 47 % мобільних додатків передають дані про географічне положення;

- 5 % посилають дані про вік, стать та інші персональні дані.

Дослідження також показало, що додатки для Apple iOS передають більше даних, ніж додатки для Android, проте цю тенденцію неможливо перевірити для всієї бази кількох сотень тисяч додатків для обох операційних систем [4].

Інші дослідження показали вразливість наступних додатків: Gmail (92% успішних атак), H&R Block (92%), Newegg (86%), WebMD (85%), CHASE Bank (83%), Hotels.com (83%). Лише захист додатків Amazon було відносно важко подолати. Для нього показник успішних атак склав менше половини – 48% [5].

3. *Використовувані раніше або непрацюючі пристрої*. У цьому випадку більшість користувачів не видаляють або не можуть видали інформацію зі свого старого мобільного пристрою належним чином та звертаються до сервісного центру, продають або викидають пристрій, не замислюючись, що наступний власник або робітник сервісного центру може легко отримати доступ до величезної кількості персональних даних. Наприклад, якщо вийшла з ладу MicroSD-пам'ять (флеш-пам'ять) для мобільних пристроїв, яка містила інформацію, більшість користувачів викидають її як непотріб, не замислюючись, що зловмисник за допомогою необхідних програмних і технічних засобів може відновити інформацію на ній.

European Union Agency for Network and Information Security (ENISA) було проведено дослідження, яке показало, що неналеж-

ним чином списані мобільні пристрої можуть привести до витоку інформації, наприклад, історія викликів, контакти, електронні листи.

4. *Фішингові атаки.* На сьогоднішній день це найбільш розповсюджений вид шахрайства. Фішинг – це вид Інтернет-шахрайства, метою якого є отримання доступу до персональних та конфіденційних даних користувача, наприклад, інформації про кредитну карту, логіни та паролі.

Одним з видів фішингової атаки є розсилка електронних повідомлень, sms-повідомлень та дзвінків від імені банків, відомих фірм та брендів, які містять у собі гіперпосилання на сайт правопорушника, що не надто відрізняється від справжнього сайту фірми, банка, бренда, пропонують взяти участь у акції або підтвердити свій логін та пароль, який користувач використовує для доступу до певного сайту, акаунтів та банківських рахунків.

5. *Атаки шпигунських програм*. Користувач, не підозрюючи, може встановити шкідливе програмне забезпечення, програми, додатки (Android.SmsSend, Android.Gongfu, Android.Plankton, Android.GoldDream, Android.Crusewind, Android.SpyEye, Android.DreamExploid, Android.Wukong, PhoneOS.HLLW.Ikee, Program.ZealSpy.1.origin, Program.LetMeSpy.1.origin та Program.CellSpy.1.origin) або заразити програмне забезпечення вірусами з web-сайтів (троянець Android.CaPson.1, банківські троянці Android.MulDrop, Android.BankBot.29. origin, Android.Banker.50.origin). Саме ці шпигунські програми надають правопорушникам повний або частковий контроль над мобільним пристроєм користувача.

У 2013 році фахівцями «Лабораторії Касперського» було виявлено близько 143 тис. нових модифікацій шкідливих програм для мобільних пристроїв, а число зразків мобільних вірусів («трояни») для крадіжки даних кредитних карт і розкрадання грошей з банківських рахунків користувачів збільшилася майже в 20 разів [6]. У свою чергу компанією Avast було проведено дослідження, яке показало, що кількість мобільних вірусів у 2014 р. в порівнянні з 2011 р. (100000 мобільних вірусів) зросла до 1 млн. [7].

У 2015 році компанією AVG було взагалі виявлено шкідливе програмне забезпечення під Android, яке здатне працювати навіть при вимкненому мобільному пристрої [8].

6. *Використання спуфінга мережі.* Хакери іноді полюють на тих, хто використовує загальнодоступні мережі Wi-Fi. Правопорушник може отримати паролі до незашифрованих веб-сайтів, пошти, передані через незашифроване з'єднання на веб-сайт тощо.

Для захисту мобільних комп'ютерних пристроїв від загроз, розглянутих вище, можна порекомендувати дотримуватись наступних правил:

1. Встановити Pin-код, пароль на телефон (або використовувати екранну блокіровку з графічним ключем), SIM-карту та карти-пам'яті.

2. Встановити антивірусні програми та постійно оновлювати їх, регулярно перевіряти мобільний пристрій на наявність вірусів.

3. Не встановлювати додатки (ігри, програми), які запитують доступ до персональної та конфіденційної інформації, та видаляти ті з них, які не використовуються.

4. Перед встановленням додатків переглядати їх рейтинги та відгуки.

5. Правильно налаштувати мобільний пристрій, оскільки він має свою систему захисту: можливість перевірки додатків на віруси та шпигунські програми, забороняти встановлення додатків з невідомих джерел, функція, яка дозволяє знайти вкрадений або втрачений мобільний пристрій.

6. Використовувати функцію, яка дозволяє або блокує доступ до Інтернету.

7. Якщо телефон містить конфіденційну інформацію, можна використовувати вбудовану функцію повного шифрування телефону або пам'яті телефону.

8. Не використовувати незахищені Wi-Fi мережі, особливо при онлайн-покупці товарів та послуг.

9. Регулярно оновлювати програмне забезпечення мобільних пристроїв з перевірених джерел.

10. Не переходити за гіперпосиланнями, які містять повідомленнях з невідомих адрес, а також не натискати на спливаючі банери та реклами.

11. Не виходити за рамки визначеної політики безпеки.

Література:

1. Мобільний комп'ютерний пристрій [Електронний ресурс]. –

Режим доступу: http://uk.wikipedia.org/wiki/ Мобільний_комп'ютер.

2. Безопасность мобильных устройств [Електронний ресурс]. – Режим доступу: http://umvs.kr.ua/bezopasnost-mobilnyh-ustrojstv-1.

3. Ваші телефони НЕ зберігають ваші секрети! [Електронний ресурс]. – Режим доступу: http://zahod.at.ua/publ/nauka/nauka/vashi_telefoni_ne_zberigajut_vashi_sekreti/10-1-0-68.

4. Исследование показало, что мобильные приложения для Android и iOS разглашают частную информацию [Електронний ресурс]. – Режим доступу: http://www.opennet.ru/opennews/art.shtml?num=29056.

5. Nealon Sean Hacking Gmail with 92 percent success / Sean Nealon [Електронний ресурс]. – Режим доступу: http://phys.org/news/2014-08-hacking-gmail-percent-success.html.

6. Смартфон расплаты: чем опасен мобильный банкинг? / Sean Nealon [Електронний ресурс]. – Режим доступу: http://bankir.ru/publikacii/s/smartfon-rasplaty-chem-opasen-mobilnyi-banking-10006094/.

7. AVAST: вредоносные программы для мобильных устройств становятся все сложнее [Електронний ресурс]. – Режим доступу: http://www.comss.info/page.php?al=vredonosnye_programmy_dlja_mobilnyh_ustrojstv_stanovjatsja_vse_slozhnee.

8. Шкідливе ПЗ шпигує за мобільним телефоном навіть після вимкнення [Електронний ресурс]. – Режим доступу: http://cikavosti.com/shkidlive-pz-shpiguye-za-mobilnim-telefonom-navit-pislya-vimknennya/