Висновки. Таким чином, у PHP 7 був прибраний застарілий код, а також було дано «зелене світло» новим можливостям і майбутнім поліпшенням в області ефективності. Плюс, PHP незабаром повинен отримати оптимізацію продуктивності. Незважаючи на часткову втрату зворотної сумісності з попередніми версіями, більшість виникаючих проблем легко вирішувані.

Бібліотеки та фреймворки мігрують на PHP 7, що призводить до появи їх нових версій. Я закликаю вас спробувати сьому версію і оцінити отримані результати. Може бути, ваш додаток вже сумісний з новою версією і готовий працювати на PHP 7, отримуючи вигоди від його використання.

Література

1. Пелещишин А.М. Позиціонування сайтів у глобальному інформаційному середовищі / А.М. Пелещишин. – Львів : Вид-во Національного університету "Львівська політехніка", 2007. – 258 с.

2. Steve Prettyman. Learn PHP 7: Object Oriented Modular Programming using HTML5, CSS3, JavaScript, XML, JSON, and MySQL. 2016. 308 p.

3. Antonio Lopez. Learning PHP 7. 2016. 414 p.

4. Mikael Olsson. PHP 7 Quick Scripting Reference, Second Edition. 2016. 136 p.

Отримана/Received : 24.4.2017 р. Надрукована/Printed :11.6.2017 р.
Рецензент: д.ф-м.н., проф.Бедратюк Л.П.

УДК 004.056

О.П. ВОЙТОВИЧ, М.В. ГУРСЬКИЙ, Л.М. КУПЕРШТЕЙН
Вінницький національний технічний університет
Д.С. СНІГОВИЙ
Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

ЗАСІБ МОНІТОРИНГУ ДЛЯ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

На основі аналізу основних методів та шляхів поширення шкідливого програмного забезпечення в ОС Android, розроблено програмний засіб для моніторингу вхідного/вихідного трафіку усіх системних та встановлених програмних застосунків.

Ключові слова: операційна система Android, загрози та вразливості, інформаційна безпека, система моніторингу, шкідливе програмне забезпечення.

O.P. VOITOVYCH, M.V. HURSKYI, D.S. SNIGOVYY
Vinnytsya National Technical University
L.M. KUPERSHTEIN
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”

MONITORING TOOL FOR ANDROID OPERATING SYSTEM

A purpose of this article is the improvement of information security of mobile devices using analysis of main threats, their ways of penetrating the system using monitoring of installed applications. Due to the high popularity of Android devices where getting root privilege’s is very simple the problem of installing software from untrusted sources and increasing the likelihood of inadvertent introduction of malicious code into mobile device is actual as never before. The problem is getting even worse with that fact that a big part of used devices are personal which means that user can use them as he want, for example, connect to production servers with trade secrets, accounting, bank accounts, etc. In this article architecture and main problems of protecting Android operation systems such as types of malware and methods of their spreading were reviewed. Based on detected ways a policy that will minimize the likelihood of malware to device and save private data from leaks was developed. One of the methods is to use monitoring software. Using it user can analyze all of the systems and minimize risks. Developed software tool allows real-time monitoring of the system and all installed applications connections to the Internet.

Keywords: operating system Android, threat and vulnerability, information security, monitoring system, malware.

Вступ

На сьогоднішній день ринок мобільних пристроїв вже обігнав ринок персональних комп’ютерів. В той же час стрімке зростання обчислювальної потужності і можливостей мобільних пристроїв ставлять нові питання і проблеми в галузі забезпечення інформаційної безпеки. Поширення мобільних пристроїв тягне за собою зростання бажаючих заволодіти як фізично цими самими пристроями, так і інформацією, яка зберігається на них. Найбільше хакерів приваблює операційна система Android в силу своєї відкритості та широкої розповсюдженості [1]. Обсяги шкідливого коду ростуть з роками майже в геометричній прогресії. У зв'язку з високою популярністю пристроїв Android, в якому отримання root-прав робиться в пару дотиків, проблема встановлення додатків з недовірених джерел, і, як наслідок, збільшення ймовірності ненавмисного впровадження шкідливого коду на мобільний пристрій, актуальна як ніколи [2].

У своїх дослідженнях В. В. Казимир та І. І. Карпачев [3] довели, що, на практиці, антивірусний захист надає обмежену безпеку, або навіть її ілюзію, а Saad M. H., Serageldin A., Salama G. [4] у своїй праці довели, що лише користувач є винним у несанкціонованому доступі до власних даних, винятком є лише вразливості у оновленнях ОС. На сьогоднішній день існує багато програмних та організаційних методів, в

яких розглядаються питання забезпечення безпеки, проте основна проблема посилюється так само тим, що значна кількість використовуваних пристроїв є особистими, а це означає, що працівник може обходитися з ним на власний розсуд, і, разом з тим, звертатися до робочих серверів з чутливими даними, таємницями, бухгалтерією, банківськими рахунками, тощо.

Метою статті є покращення стану інформаційної безпеки мобільних пристроїв, шляхом аналізу головних загроз, способів їх проникнення в систему за рахунок моніторингу та аудиту програмних додатків, встановлених на мобільних пристроях.

Аналіз ОС Android

ОС Android за невеликий проміжок часу стала однією з найпопулярніших систем для різноманітних мобільних пристроїв [1]. Її використовують як великі виробники зі світовим ім'ям, так і невеликі компанії, тому ціновий діапазон готової продукції, такої як смартфони і планшетні комп'ютери, дозволяє задовольнити потреби споживачів практично на сто відсотків. Саме широкий асортимент, гнучке ціноутворення та підтримка платформи з боку значного числа виробників стали одними з головних чинників успіху і дозволили системі зайняти нинішній стан на ринку.

Однак така величезна кількість користувачів просто не могла залишитися без уваги з боку зловмисників. Побудувавши на розробці і поширенні шкідливих програм цілу індустрію зі своїми законами, вони стали вкрай небайдужі до будь-яких джерел легкої наживи. Разом із розвитком технологій створюються нові типи шкідливого програмного забезпечення. Більша частина ШПЗ створюється як для розповсюдження реклами, так і використовуючи вразливості у системі або неуважність користувача, для серйозних атак, наприклад на системи мобільного банкінгу або проникнення у корпоративні системи. На рис. 1 зображено найбільш розповсюджені типи ШПЗ за 2015-2016 рр. [2].

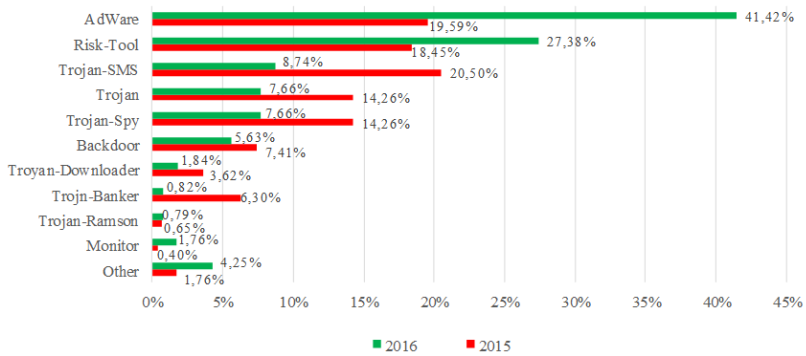


Рис. 1. Розподілення мобільних загроз за типами за 2015-2016 рр.

Таке розповсюдження ШПЗ розробленого під ОС Android зумовлено, зокрема, архітектурою (рис. 2).

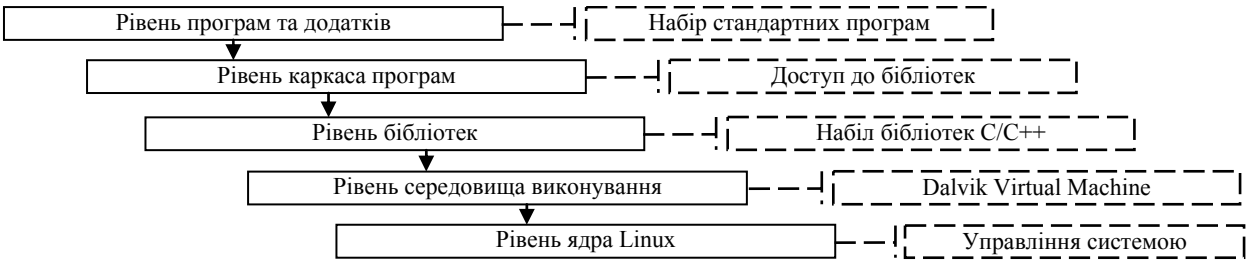


Рис. 2. Архітектура ОС Android

Архітектура ОС Android побудована таким чином, що всі програми працюють з обмеженими правами і не мають доступу до захищених даних інших додатків [5].

На рівні ядра розташовуються основні служби управління процесами, пам'яттю, файлової системою. Хоча і створено ядро Android на ядрі Linux, сама ж система Android не є чистою Linux-системою, вона містить деякі відмінності і має додаткові специфічні розширення ядра - власні механізми розподілу пам'яті, взаємодії процесів тощо [5].

Середовище виконання – це віртуальна машина DalvikVirtualMachine, яка грає роль деякого шлюзу. Дозволяє програмам отримувати доступ до кореневих бібліотек ОС Android, забезпечуючи тим самим необхідну функціональність Java-програм [6]. Хоча Dalvik VM істотно відрізняється від Java VM. Над системними бібліотеками і функціональними бібліотеками віртуальної машини розташовуються основні служби управління операційної системи. Це так звані «менеджери», кожен з яких відповідає за свої операції, використовувані програмами. Виконувані програми можуть включати в себе набір менеджерів взаємодії (менеджери діяльності, пакетів, вікон, ресурсів тощо) [7].

Набір бібліотек C/C++, таких як OpenGL, SGL 2-D графіки, WebKit, бібліотеки шрифтів, SSL,

бібліотеки підтримки libc, баз даних SQLite і мультимедіа-бібліотек (MediaFramework) використовуються різними компонентами ОС Android. Їх ще називають «кореневими бібліотеками» [8].

Використання каркаса додатків ApplicationFramework дозволяє отримати розробникам доступ до функцій цих бібліотек, основними з яких є SSL (забезпечує безпечну передачу даних по мережі) та MediaFramework (потрібні для реалізації задач запису та відтворення аудіо- та відеоконтенту).

Під рівнем додатків мається на увазі набір стандартних програм для пристроїв, за допомогою яких можна здійснювати основні характерні для них операції: програма для управління контактами, телефонії і SMS, поштовий клієнт, вбудований браузер, програми для визначення місця розташування, пошуку адрес на карті, калькулятор, органайзер тощо [9].

Однією з особливостей ОС Android, яка зумовлює проблеми з безпекою, є те, що стандартні програми не відрізняються пріоритетом від стороннього ПЗ призначеного для користувача рівня додатків, а тому перші можна замінити альтернативними, на свій смак, проте такий підхід дозволяє зловмисникам впроваджувати ШПЗ у ОС Android і отримувати ті самі права, що і легальне ПЗ.

Шляхи потрапляння ШПЗ можуть бути різними (рис. 3): від звичайного SMS-повідомлення до заздалегідь розробленої та точної атаки на конкретну людину.

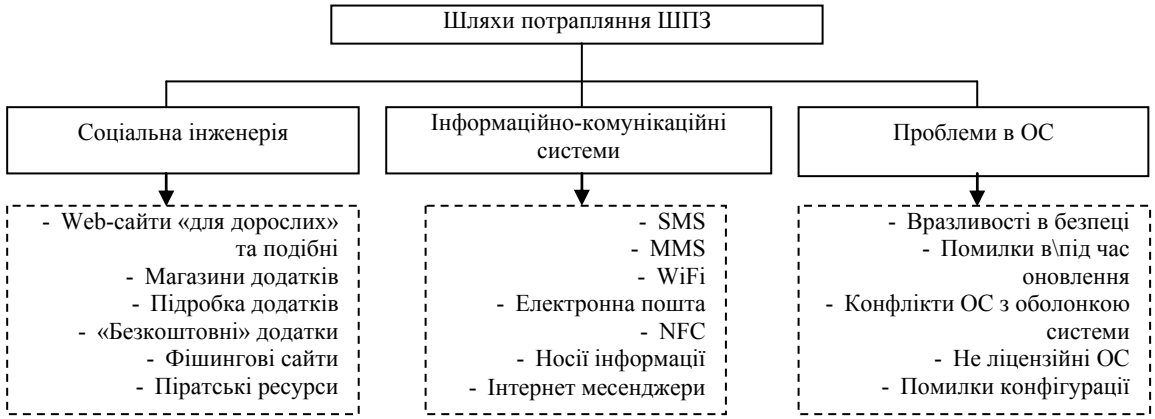


Рис. 3. Шляхи потрапляння ШПЗ на Android-пристрій

Щороку з'являються нові технології, які впроваджуються розробниками пристроїв та активно використовуються користувачами в подальшому. Кожна така технологія не може одразу тестуватися в усіх ймовірних сценаріях роботи, тому, зазвичай, саме в них міститься найбільша кількість вразливостей. Також, часто розробники встановлюють поверх самої ОС Android власну графічну оболонку з ексклюзивними налаштуваннями та функціями, які можуть суперечити політиці Google та конкурувати з їх сервісами [10]. Проте найбільш небезпечними залишаються методи соціальної інженерії, оскільки вони опираються на психологічні особливості людини. Часто, отримуючи ту чи іншу інформацію за допомогою різних сервісів миттєвих повідомлень, можна також отримати небажаних «гостей» на власний пристрій. Велику небезпеку становлять публічні або недовірені мережі, оскільки будь-хто може перехоплювати або змінювати інформацію під час сеансу [11].

Після потрапляння будь-якого ШПЗ на Android-пристрій, жертва ще довго може нічого не знати про це. Більшість таких додатків маскуються та чекають нагоди для виконання своїх задач. Так, деякі з них, можуть при підключенні до мережі Інтернет одразу надіслати вкрадену конфіденційну інформацію, а інші чекають, наприклад, поки користувач не використає свої банківські реквізити.

Можна виділити декілька факторів, які допоможуть визначити, що пристрій було уражено [8, 9, 11–13]: великі рахунки за телефон(SMS, MMS, трафік тощо), обмеження доступу до даних, витрати мережевого трафіку, великі витрати заряду акумулятора, увімкнення сервісів без відома власника, зниження продуктивності пристрою, велика кількість реклами, поява великих банерів з різними вимогами оплати, постійні помилки та припинення роботи додатків, неможливість увімкнення/вимкнення окремих функцій пристрою, поява незнайомих додатків, неможливість видалення додатків.

Однією з головних проблем безпеки при роботі з ОС Android, завжди залишався людський фактор. Якою б захищеною не була операційна система, безтурботність, неуважність, самовпевненість і проста необізнаність рано чи пізно може зіграти поганий жарт з користувачем. Наприклад, впевненість користувача в тому, що йому нічого не загрожує, змушує його ігнорувати засоби безпеки, такі як додатки з невідомих джерел. У разі застосування зловмисниками привабливих пропозицій, наприклад, завантаження безкоштовних версій платних додатків та ігор, використовується прагнення людей отримати вигоду без втрат для себе. Коли підробляється відомий сайт, гра або додаток, а користувач при цьому недосвідчений, він може і не усвідомлювати, що піддається якомусь ризику, встановлюючи ту чи іншу програму або вводячи свою конфіденційну інформацію. Само по собі ШПЗ не може потрапити на пристрій жертви, тому в своєму арсеналі зловмисники завжди мають методи соціальної інженерії [12].

Відомо, що антивірусні засоби в ОС Android не завжди виконують поставлені на них задачі, а за часто і самі містять функції шкідливого програмного забезпечення [7]. Найбільш дієвим захистом є

уважність користувача, адже саме він завантажує та дозволяє, в тому числі, підозрілі функції. Для того, щоб уникнути зараження ШПЗ в першу чергу необхідно дотримуватися таких рекомендацій [12–14]:

- не переходити за невідомими джерелами, особливо тим, які отримали в SMS, е-пошті тощо;
- не встановлювати недовірені («кастомні») прошивки;
- без необхідності та досвіду, не отримувати права суперкористувача;
- увімкнути функції «Блокування повторної активації» та «Заборона додатків з невідомих джерел»;
- користуватися перевіркою безпеки додатків Google;
- вимикати послугу автоотримання MMS;
- перевіряти права доступу при встановленні додатків;
- завжди встановлювати найактуальніші оновлення;
- не вмикати функцію «автоплатіж» з банківських, чи інших карт;
- не користуватися публічними або недовіреними мережами;
- періодично робити backup важливої інформації;
- використовувати шифрування;
- використовувати засоби для моніторингу.

Якщо ж ШПЗ потрапило на пристрій, в залежності, що це саме за додаток, є різні методи його видалення, але найбільш дієвим завжди було та є повне скидання до заводських налаштувань.

Розробка засобу для моніторингу

Хоч і антивіруси не в змозі повністю захистити від ШПЗ, але деякі типи програмного засобу допоможуть у виявленні таких додатків, а саме засоби моніторингу процесів та ресурсів [14].

Засоби для моніторингу призначені для того, щоб в режимі реального часу можна було бачити, що відбувається з системою та її складовими. Наприклад, моніторинг використання пам'яті, енергій акумулятора, активності тощо. Часто записи здійснені під час моніторингу використовують при поломці або у випадку некоректної роботи пристрою. Моніторинг може бути активним і пасивним, під час якого здійснюється цілодобове спостереження та логування усіх дій системи, від зміни файлу до перепадів температури акумулятора, для подальшого аудиту. Активний моніторинг передбачає імітацію реального втручання або атаки на систему [15].

Саме тому, що системи моніторингу здатні слідкувати за будь-якими діями та змінами в системі, вони є найбільш дієвим засобом захисту від зламу мобільних пристроїв.

Розроблений засіб для моніторингу дозволяє отримувати інформацію про вхідний/вихідний трафік кожного системного або встановленого додатку з правами на використання мережі Інтернет. Більшості ШПЗ потрібно мати вихід до мережі для завантаження додатків, файлів, отримання інструкцій від розробника, передавання конфіденційної інформації тощо.

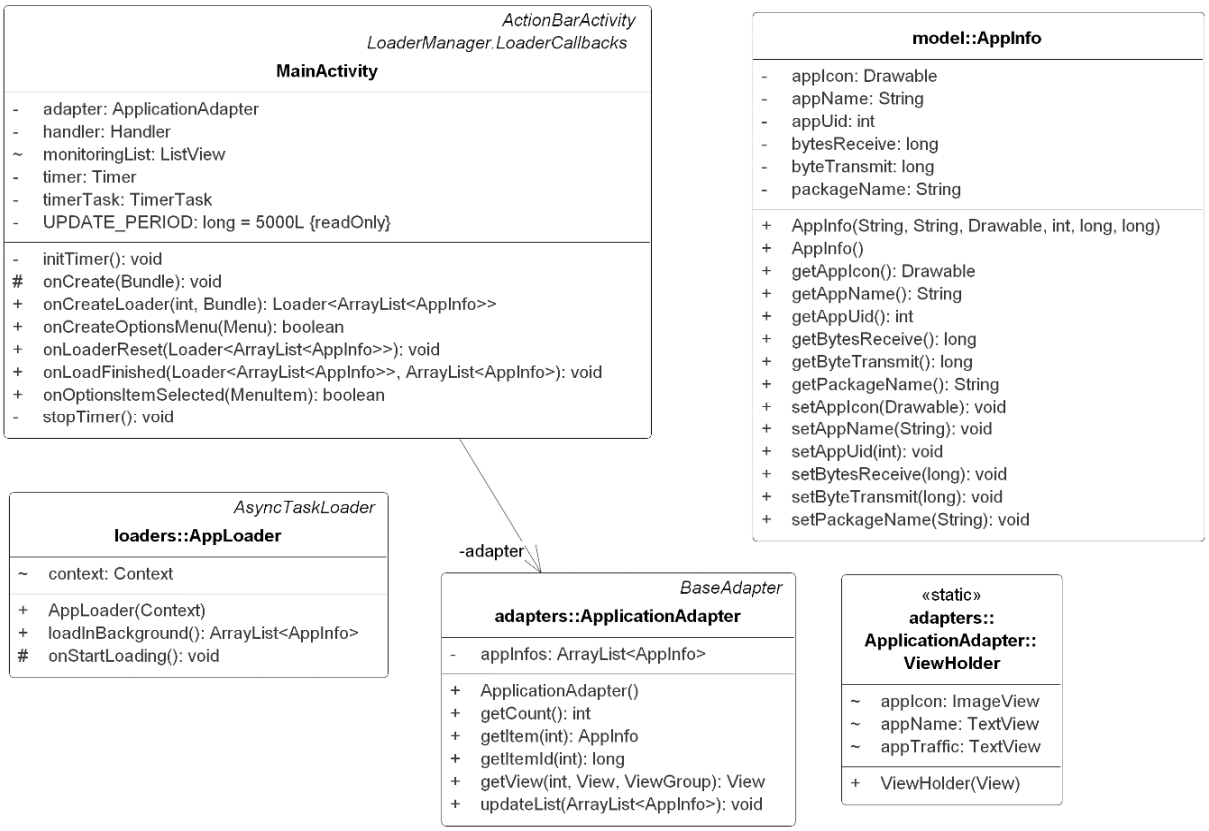
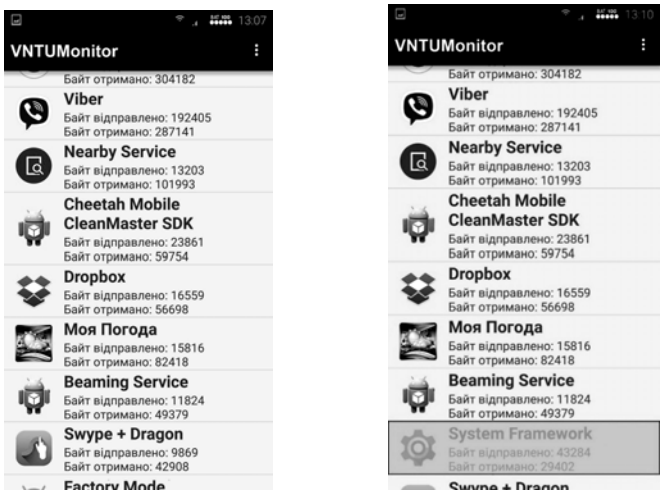


Рис. 4. UML-діаграма додатку для моніторингу

Для роботи програмному засобу для моніторингу необхідно отримати від операційної системи повний список усіх встановлених та системних програмних пакетів. Для аналізу отриманого списку додатків на наявність у них прав для доступу до мережі Інтернет, програмний засіб звертається до менеджеру додатків із запитом перевірки системи дозволів кожного додатку. Отримавши інформацію, формується новий список, в якому відсіюються додатки без доступу до мережі Інтернет, і потім виводиться у сортованому вигляді на інтерфейс користувача та додається інформація про вхідні/вихідні дані кожного додатку. UML-діаграму розробленого додатку зображено на рис. 4.

Відповідно до структури, додаток поділено на частини (модулі), в яких відбуваються спеціалізовані процедури. В класі MainActivity відбувається пошук додатків, ініціалізація таймерів, слухачів, завантажувачів, прив'язка графічної частини до коду і вся обробка даних. В класі AppLoader відбувається пошук додатків, які використовують мережу Інтернет в окремому потоці. Клас ApplicationAdapter виконує обробку даних для створення списку. Клас ViewHolder формує і обробляє кожен елемент списку. Клас AppInfoце аналог класуPOJO, тобто клас створений лише для збереження даних (Data class).

Розробка даних програмних продуктів була проведена за допомогою об'єктно-орієнтованої мови програмування Java у середовищі програмування AndroidStudio. Після встановлення та запуску, додаток автоматично відфільтрує та відсортує усі програмні засоби та відобразить їх у зручній для користувача формі (рис. 5, а).



а) **б)**

Рис. 5. Вигляд вікна з функціонуванням додатку
(а – при запуску додатку; б – із появою нового шпигуна)

Для тестування було створено програмний засіб для несанкціонованого отримання конфіденційної інформації. Додаток створений без інтерфейсу, не відображається у «Меню додатків» пристрою та має системну назву та іконку. Після встановлення, засіб одразу передає конфіденційну інформацію на сервер.

Кожного разу, після запуску додатку для моніторингу відбувається повторна перевірка системи на наявність нових додатків. Якщо такі є, то, для зручності аналізу, такі додатки підсвічені іншим кольором. Як видно із рис. 5, б, новий додаток було одразу ідентифіковано.

Таким чином, разом із користувачем, додаток може забезпечити досить надійний захист від несанкціонованого доступу до персональних даних. Звісно від зараження пристрою, крім людської уважності, не може захистити нічого, але, якщо все ж таке станеться, то розроблений програмний засіб допоможе знайти та позбутися шкідливого додатку.

Висновки

Отже, було розглянуто основні проблеми захисту ОС Android, а саме види шкідливого програмного забезпечення та способи їх поширення. На основі виявлених причин розроблено рекомендації, дотримання яких дозволить зменшити ймовірність потрапляння ШПЗ на пристрій та зберегти конфіденційні дані від витоку. Показано, що існуючі методи не можуть гарантувати повної захищеності, оскільки однією з головних проблем безпеки при роботі з ОС Android є людський фактор. Якою б захищеною не була операційна система, безтурботність, неуважність, самовпевненість і проста необізнаність рано чи пізно піддає небезпеці власника смартфону. Будь-який ліцензійний, або навіть додаток для захисту самого ж пристрою, може нести в собі додаткову приховану функцію.

Одним із методів вирішення проблеми є використання програм-моніторів. З їх допомогою користувач може самостійно аналізувати усі дії системи. Реалізований програмний засіб дозволяє у режимі реального часу слідкувати за доступом до мережі Інтернет усіх встановлених та системних додатків. Це дає можливість проведення аудиту інформаційної безпеки мобільного пристрою та дослідження комп'ютерних інцидентів.

Література

1. AndroidSecurityBulletin — January 2017 [Електронний ресурс]. – Режим доступу : https://source.android.com/security/bulletin /2017-01-01.html – Назва з екрану

2. Мобильные вирусы и угрозы. Статистика [Електронний ресурс]. – Режим доступу : http://www.kaspersky.ua/internet-security-center/threats/mobile/

3. Karpachev I., Kazymyr V. Functional security in an ANDROID mobile architecture / I. Karpachev, V. Kazymyr // Вісник Чернігівського державного технологічного університету. – 2015. – № 1 (77).

4. Saad M. H., Serageldin A., Salama G. I. Android spyware disease and medication / M. H. Saad, A. Serageldin, G. I. Salama // Information Security and Cyber Forensics (InfoSec), 2015 Second International Conferenceon. – IEEE, 2015. – С. 118–125.

5. Mark L. Murphy. The Busy Coder's Guideto Android Development / Mark L. Murphy // Commonsware, LLC. – 2013. – 443 p.

6. Understanding security on Android. URL: http://www.ibm.com/developerworks/library/x-androidsecurity.

7. Fedler R. Android OS security: risks and limitations / R. Fedler, C. Banse, C. Kraub, V. Fuesing. – 2012. – P. 19–27.

8. Mobile application security on android, context on android security / J. Burns // BlackHat. – 2009. – 27 p.

9. Ratazzietal P. A systematic security evaluation of android's multiuser framework / P. Ratazzietal // Proc. IEEE MoST, 2014. – P. 1–10.

10. Fedler R. Effectiveness of malware protection on android and evaluation of android antivirus apps / R. Fedler, J. Schutte, M. Kulicke // Applied and integrated security. – 2014. – P. 7–13, 26–32.

11. Мелешко О. О. Способи захисту інформації з обмеженим доступом в мобільних пристроях від витоку / О. О. Мелешко, О. С. Болотнікова // Сучасний захист інформації. – 2016. – № 1.

12. Войтович О. П. Дослідження інцидентів безпеки в ОС Android / О. П. Войтович, М. В. Гурський // Тези доповідей XLV Науково-технічної конф. Вінницького національного технічного університету / ФІТКІ – Вінниця, 2016.

13. Вирусология от SAMSUNG [Електронний ресурс]. – Режим доступу : http://www.samsung.com/ru/support/skp/faq/1095966 – Назва з екрану

14. Zhou Y. Dissecting android malware: Characterization and evolution / Y. Zhou, X. Jiang // Security and Privacy (SP), 2015 IEEE Symposiumon. – IEEE, 2015. – С. 95–109.

15. Мельников Д. А. Информационная безопасность открытых систем : учебник / Мельников Д. А. – М. : ФЛИНТА, 2013. – 442 с.

Отримана/Received : 9.5.2017 р. Надрукована/Printed :11.6.2017 р.
Рецензент: д.т.н., проф. Мартинюк Т.Б.