УДК 004.56

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ МОБІЛЬНИХ ПРИСТРОЇВ ВІД ЗАГРОЗ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ

Сурм'як І.О.
Тернопільський національний економічний університет, магістрант

I. Вступ

Незважаючи на удосконалення технологій в області захисту інформації, вразливість персональних мобільних пристроїв продовжує зростати. На сьогоднішній день найбільш поширеними загрозами для персональних мобільних пристроїв є: впровадження шкідливого коду через недостовірні джерела, атаки через веб-додатки, атаки з використанням методів соціальної інженерії, загрози цілісності та конфіденційності даних.

II. Мета роботи

Метою роботи є формування рекомендацій щодо захисту персональних мобільних пристроїв від загроз несанкціонованого доступу.

III. Особливості захисту персональних мобільних пристроїв

Розглянувши сучасні підходи щодо забезпечення захисту від несанкціонованого доступу можна відмітити спільну позицію у них, щодо реалізації системного підходу, який включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, і т.д.). Комплексний характер захисту виникає з комплексних дій зловмисників, які прагнуть будь-якими засобами отримати важливу для них інформацію.

У роботі сформовано рекомендації щодо використання різних методів для захисту конфіденційної інформації від несанкціонованого доступу в процесі її передачі і зберігання, які можна використовувати при побудові комплексного підходу щодо захисту персональних мобільних пристроїв.

Наведемо перелік рекомендованих методів:

- приховати канал передачі інформації, використовуючи нестандартний спосіб передачі повідомлень або VPN;
- замаскувати канал передачі закритої інформації в відкритому каналі зв'язку, наприклад, сховавши інформацію в стеганографічному контейнері;
- ускладнити можливість перехоплення зловмисником переданих повідомлень, використовуючи спеціальні методи передачі по широкосмугових каналах сигналу під рівнем шумів або з використанням «стрибаючих» несучих частот;
- використовувати криптографічні перетворення.
- встановлювати додатки для захисту від шкідливого програмного забезпечення;
- використовувати персональний брандмауер для захисту інтерфейсів пристрою.

Висновок

У роботі виявлено існуючі загрози інформаційної безпеки для персональних мобільних пристроїв. Запропоновано рекомендації для захисту конфіденційної інформації від несанкціонованого доступу в процесі її передачі і зберігання, які можна використовувати при побудові комплексного підходу щодо захисту персональних мобільних пристроїв.

Список використаних джерел

1. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: НТ, 2004. 384 с.
2. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2005.
3. Барсуков, В. С. Безопасность: технологии, средства и услуги / В. С. Барсуков. – М. : КУДИЦ-ОБРАЗ, 2001. – 496 с
4. Neidhardt, E. Asymmetric Cryptography for Mobile Devices / E. Neidhardt. – Service-centric Networking, 2011. – P. 1-12.
5. Доклад «Мобильные угрозы 2010/2011» [Электронный ресурс]. – Режим доступа к ресурсу: http://www.juniper.net.
6. Сайт SecureList [Электронный ресурс]. – Режим доступа к ресурсу: http://www.securelist.com/
7. McAfee Threats Report: Second Quarter 2015 [Электронный ресурс]. – Режим доступа к ресурсу: http://www.mcafee.com