Teresa Mendyk-Krajewska, Zygmunt Mazur, Hanna Mazur

Dostępność zasobów internetowych z wykorzystaniem urządzeń mobilnych

Ekonomiczne Problemy Usług nr 104, 229-237

2013

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 762 EKONOMICZNE PROBLEMY USŁUG NR 104 2013

TERESA MENDYK-KRAJEWSKA, ZYGMUNT MAZUR, HANNA MAZUR
Politechnika Wrocławska

DOSTĘPNOŚĆ ZASOBÓW INTERNETOWYCH Z WYKORZYSTANIEM URZĄDZEŃ MOBILNYCH

Wprowadzenie

Atrakcyjność mobilnego dostępu do zasobów sieci globalnej i wynikające z tego ogromne zainteresowanie użytkowników bezprzewodowymi rozwiązaniami spowodowały dynamiczny ich rozwój. Sprzedaż urządzeń mobilnych nieustannie rośnie kosztem tradycyjnych komputerów osobistych. Dzięki nowym technologiom dostęp do Internetu z wykorzystaniem urządzeń mobilnych (telefonów komórkowych, smartfonów, tabletów, palmtopów, notebooków) stał się szybki i wygodny. Poszczególne urządzenia, różniące się między sobą budową, wielkością, sposobem interakcji z użytkownikiem i coraz bardziej rozbudowywaną funkcjonalnością, są wykorzystywane do komunikacji, realizacji różnego rodzaju usług oraz zadań biznesowych. Jakość bezprzewodowego dostępu do Internetu jest także zróżnicowana, zależna od lokalnych dostawców usług sieciowych.

Przewiduje się, że w niedługim czasie połączenia z siecią globalną będą realizowane głównie przy pomocy smartfonów. Z badań firmy Ericsson Consumer Lab wynika, że w Polsce użytkownicy mobilnego dostępu do Internetu stanowią już ponad połowę wszystkich internautów[1]. Jak dotąd większość z nich wykorzystuje do tego laptopy i netbooki, jednak udział smartfonów systematycznie rośnie. W 2011 roku sprzedaż smartfonów na świecie przekroczyła 487 milionów egzemplarzy, zaś w Polsce ich odsetek w stosunku do wszystkich telefonów komórko-

[1] T. Kutera: *Jak Polacy łączą się z siecią?*, 24.11.2011.

wych wyniósł 24% i nadal rośnie[2]. Tylko w trzecim kwartale 2012 roku na całym świecie sprzedano ich prawie 170 milionów[3].

Ogromna popularność urządzeń mobilnych, zwłaszcza rozwój funkcjonalności smartfonów, spowodowała pojawianie się dla nich coraz większej liczby szkodliwych kodów. Pomimo to wielu użytkowników korzysta z nich jak ze zwykłych telefonów, bez świadomości zagrożenia, nie stosując odpowiednich zabezpieczeń.

1. Technologie łączności bezprzewodowej

Technologie komunikacji bezprzewodowej są systematycznie rozwijane. W efekcie prowadzonych prac badawczych (dotyczą głównie poprawy parametrów transmisji i wzrostu bezpieczeństwa) opracowywane są nowe standardy.

Najpopularniejszym systemem telefonii komórkowej na świecie jest GSM (*Global System for Mobile Communications*), który obejmuje ok. 80% światowego rynku. Pomimo opracowania nowszych technologii sieci te są nadal rozwijane ze względu na obszar dostępności systemu i liczbę abonentów. Do czasu gdy systemy nowej generacji zastąpią wykorzystywane rozwiązania, dla zapewnienia ciągłości usług (transmisja głosu i danych, wiadomości SMS i MMS, dostępność Internetu), gwarantuje się ich wzajemną współpracę. Obecnie usługi z wykorzystaniem technologii GSM świadczy ponad 700 operatorów w ponad 200 krajach i terytoriach zależnych (istotny wyjątek stanowi Japonia). W Polsce sieć jest dostępna od września 1996 roku; jesienią 2012 roku usługi w standardzie GSM świadczyło czterech operatorów (sieci: T-Mobile, Plus, Orange i Play). Wyróżnia się pięć głównych standardów: GSM 850 i GSM 1900 – używane w większości krajów Ameryki Północnej i Południowej, standardy GSM 900/1800 – stosowane przez pozostałe kraje oraz GSM 400, który można wykorzystywać do pokrycia obszarów niezamieszkałych.

Systemy telefonii komórkowej GSM drugiej generacji, z dominującą usługą transmisji głosu, rozwinięte zostały o pakietowy przesył danych. Telefonia komórkowa trzeciej generacji integruje wszystkie systemy komunikacyjne: teleinformatyczne, radiowe i telewizyjne. Bazuje na standardzie UMTS (*Uniwersal Mobile Telecommunications System*) i umożliwia przesył danych w trybie pakietowym oraz pełnoprawną (obok transmisji dźwięku) realizację usług wykorzystujących transmisję wideo. Nowszym standardem jest LTE[4], oparty o technologie OFDM (*Orthogonal Frequency-Division Multiplexing*)[5] i SC-FDMA (*Single Carrier – Frequency*

---

[2] www.orange.pl/ocp-http/PL/Binary2/1979463/4053940725.pdf.

[3] http://pclab.pl/news51648.html [dostęp 16.11.2012].

[4] *Long Term Evolution* – pierwsza wersja standardu z 2008 roku; LTE-Advanced z 2010 r. jest zgodna ze zbiorem wymagań dla czwartej generacji sieci radiowych IMT-Advanced.

[5] Do transmisji danych od stacji bazowej do urządzenia mobilnego.

Division Multiple Access)[6], który między innymi wprowadza większą prędkość przesyłu danych oraz mniejsze opóźnienia i koszty transmisji.

Do głównych standardów bezprzewodowych sieci komputerowych Wi-Fi[7] należą: 802.11a (5 GHz, 54 Mb/s), 802.11b (2,4 GHz, 11 Mb/s), 802.11g (2,4 GHz, 54 Mb/s), 802.11n (5 GHz, 300 Mb/s oraz 2,4 GHz, 150 Mb/s) i 802.11ac (5 GHz, 1 Gb/s). Technologia Wi-Fi umożliwia korzystanie z darmowego Internetu poprzez punkty dostępowe (hotspoty) lokalizowane w powszechnie uczęszczanych miejscach. Technologia ta może też stanowić uzupełnienie dla sieci GSM. Istnieją firmy (np. Zyxel, SocketIP, Unitech), które oferują oparte na niej usługi telefoniczne.

2. Funkcjonalność i wykorzystanie urządzeń mobilnych

Nowoczesne urządzenia mobilne charakteryzuje rozbudowana funkcjonalność. Zaawansowane technicznie, pozwalają na prowadzenie tych samych działań co podłączone do sieci komputery stacjonarne. Umożliwiają przeglądanie stron WWW, korzystanie z poczty elektronicznej i sieci społecznościowych, przesyłanie plików, oglądanie filmów, realizację usług bankowych, zakupy online, używanie usług lokalizacyjnych, a także robienie filmów i dobrej jakości zdjęć. Specyficzne wymagania stawia współczesnym urządzeniom segment biznesowy, dlatego nowsze modele oferują dodatkowo tak zaawansowane funkcje, jak zarządzanie informacjami czy odczytywanie dokumentów biurowych w różnych formatach.

Na szczególną uwagę zasługują smartfony i tablety, których używanie staje się niezwykle popularne. Smartfony to urządzenia lżejsze niż iPady[8], łączące w sobie funkcje telefonu komórkowego i palmtopa (PDA[9]). W 2010 roku (gdy firma Apple zaprezentowała iPada) sprzedaż smartfonów po raz pierwszy przewyższyła sprzedaż komputerów[10]. Tablety to urządzenia większe niż telefony czy palmtopy, wyposażone w duży ekran dotykowy (z zastosowaniem technologii Multi-Touch), port USB oraz karty do łączności bezprzewodowej (Wi-Fi, GSM, 3G, 4G). Oferują możliwość oglądania filmów i zdjęć, dostęp do Internetu oraz część funkcji nowoczesnych telefonów komórkowych.

Możliwości urządzenia mobilnego, wygoda użytkowania oraz bezpieczeństwo danych w dużej mierze zależą od systemu operacyjnego. Zestawienie popularności

---

[6] Dla transmisji danych od urządzenia do stacji bazowej.

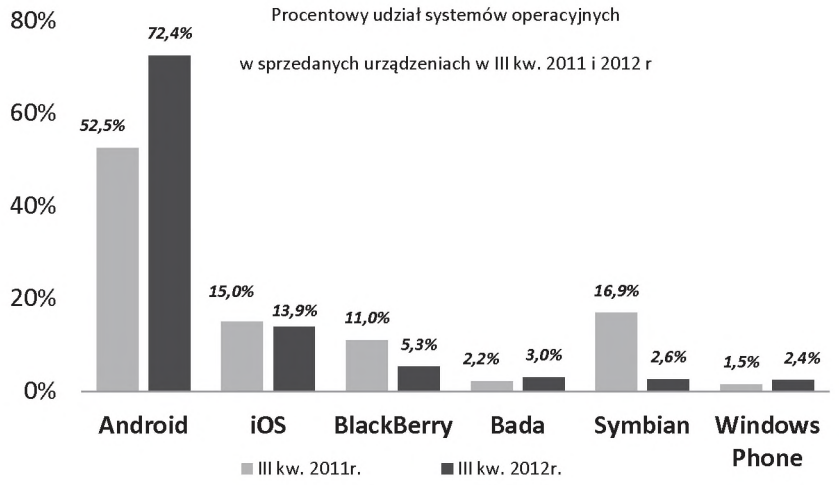
[7] *Wireless Fidelity* – potoczna nazwa technologii bezprzewodowej – standardy IEEE 802.11.

[8] iPad – tablet firmy Apple, większy od iPhone'a i telefonu komórkowego.

[9] *Personal Digital Assistant* – komputer kieszonkowy, mniejszy od laptopa czy netbooka; łączność z innymi urządzeniami przez IrDA, Bluetooth i Wi-Fi.

[10] http://technologie.gazeta.pl/internet/1,113841,12828126,Historia_zatoczyla_kolo___triumfalny_powrot_tabletow.html.

systemów operacyjnych urządzeń mobilnych w III kwartale w latach 2011 i 2012, według danych firmy analitycznej Gartner przedstawiono na rysunku 1.



Rys. 1. Popularność systemów operacyjnych w III kwartale w latach 2011 i 2012

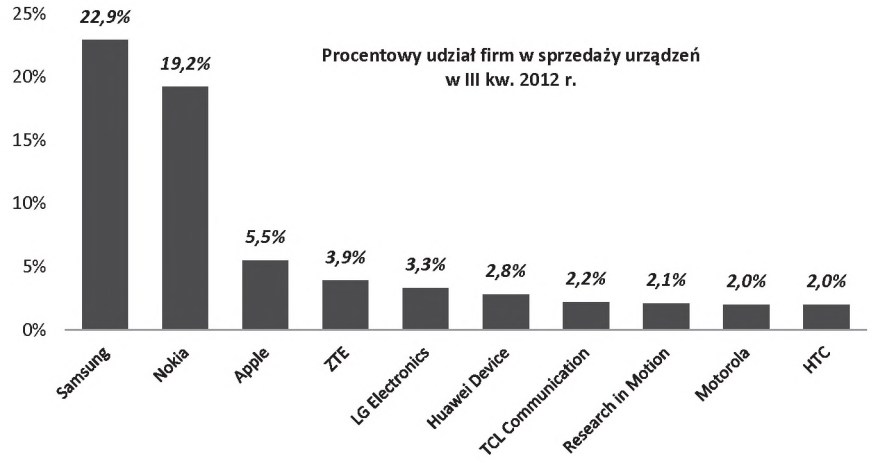
Źródło: Opracowanie własne na podstawie: pclab.pl/news51648.html

Z przedstawionych danych można zaobserwować znaczący spadek sprzedaży urządzeń z systemem Symbian (z 16,9% do 2,6%) oraz wzrost zainteresowania urządzeniami z systemem Android (z 52,5% do 72,4%). Popularne są też systemy iOS, BlackBerry OS i Bada OS, natomiast sprzedaż innych systemów jest niewielka i wykazuje tendencję spadkową (z 0,9% w III kw. 2011 r. do 0,4% rok później). Dalekie miejsce zajmowane przez Windows Phone firmy Microsoft może nie dziwić wobec problemów (np. samoczynne restarty) zgłaszanych przez użytkowników smartfonów wyposażonych w jego najnowszą wersję Windows Phone 8.

Zainteresowaniem użytkowników cieszą się urządzenia takich firm jak Samsung, Nokia, Apple, ZTE i LG Electronics. Procentowy udział w sprzedaży telefonów komórkowych i smartfonów popularnych producentów sprzętu w III kwartale 2012 roku przedstawiono na rysunku 2. Na pierwszym miejscu listy znalazła się firma Samsung z wynikiem poniżej 25%, udział innych firm, nieobjętych wykresem, to 36,2% – zatem trudno wskazać lidera.

Z badań firmy doradczej Ernst & Young przeprowadzonych na przełomie maja i kwietnia 2012 roku wynika, że użytkownicy smartfonów korzystają z niewielkiej liczby oferowanych usług (najczęściej dodatkowo jest to przeglądanie stron

WWW, korzystanie z mediów społecznościowych i usług muzycznych) z obawy przed zapłaceniem wysokich rachunków[11].



Rys. 2. Popularność producentów urządzeń mobilnych w III kwartale 2012 roku według liczby sprzedanych egzemplarzy

Źródło: opracowanie własne na podstawie: pclab.pl/news51648.html.

Badaniem objęto 6000 klientów sieci komórkowych w 12 krajach – co piąty ankietowany czuł się niedoinformowany w zakresie planów taryfowych mobilnego Internetu oferowanych przez operatora sieci komórkowej.

3. Zagrożenia dla urządzeń mobilnych

Zagrożenie dla urządzeń mobilnych rośnie wraz z ich popularnością. Użytkownicy często przechowują w nich ważne i poufne dane, co jest przyczyną zainteresowania nimi przestępców sieciowych. Im większa funkcjonalność urządzenia, tym większe konsekwencje w przypadku jego zawirusowania lub utraty.

Gwałtowny wzrost zagrożenia dla bezpiecznego ich użytkowania zaobserwowano w 2010 roku. Od tego czasu zidentyfikowano już tysiące różnego typu szkodliwych kodów i wiele sposobów przeprowadzania ataków. Nie różnią się one od zagrożeń dla konwencjonalnych komputerowych systemów informatycznych. Można wśród nich wymienić: pobieranie z sieci szkodliwych kodów, blokowanie karty

[11] http://ey.media.pl/pr/226896/uzytkownicy-smarfonow-nie-wykorzystuja-ich-potencjalu-boja-sie-wyzszych-rachunkow [dostęp 7.11.2012].

pamięci lub całego urządzenia, modyfikowanie i usuwanie danych lub ich nieuprawnione pozyskiwanie (np. haseł uwierzytelniających do przeprowadzenia transakcji bankowych), automatyczne wymuszanie połączeń międzynarodowych o wysokiej odpłatności, a nawet zdalne udostępnianie zainfekowanego urządzenia.

Szkodliwe programy są rozprzestrzeniane różnymi drogami, między innymi przy pomocy MMS-ów i SMS-ów, z wykorzystaniem technologii Bluetooth czy portali internetowych. Nieautoryzowany dostęp do urządzeń mobilnych umożliwiają też błędy występujące w ich oprogramowaniu systemowym. Szkodliwe programy są rozpowszechniane nawet przez firmowe sklepy internetowe, takie jak Apple App Store czy Google Play, gdzie kontrola udostępnianych aplikacji jest niedostateczna. Analiza dokonana przez firmę BT zajmującą się bezpieczeństwem danych wykazała, że w Google Play około 33% oferty sklepu zawierało niebezpieczny kod[12].

Najbardziej zagrożone są urządzenia z systemem Android, z powodu zbyt rzadkiej aktualizacji oprogramowania i niskiego poziomu zabezpieczeń. W 2011 roku wykryto prawie trzykrotnie więcej kierowanych na nie zagrożeń niż w ciągu wcześniejszych sześciu lat łącznie[13].

Jedno z pierwszych poważnych zagrożeń stanowiło stworzenie witryny jailbreakme.com wykorzystującej luki w systemie operacyjnym Apple'a, za pośrednictwem której można było zdjąć blokadę z iPhone'a[14], iPada lub iPoda Touch[15]. W tym samym czasie użytkownicy systemu Android byli atakowani przez konia trojańskiego Tap Snake, który symulując popularną grę, umożliwia szczegółowe odtworzenie trasy urządzenia. Innym głośnym przykładem zagrożenia jest aplikacja ZeuS przechwytująca wiadomości SMS z jednorazowymi hasłami do autoryzacji transakcji bankowych dokonywanych online, który to sposób przekazywania poufnych danych uchodził dotąd za jedno z najwygodniejszych i najbezpieczniejszych rozwiązań bankowości elektronicznej.

Jesienią 2012 roku informowano o wykryciu poważnych luk w zabezpieczeniach iPhone'a 4S (iOS 5.1.1) i 5 (iOS6) oraz Samsunga Galaxy S3 (Android 4.0.4)[16]. W pierwszym przypadku uruchomiony exploit, wykorzystując wadę przeglądarki Safari, umożliwia pozyskanie danych: historii wyszukiwania, listy kontaktów i zdjęć, w drugim – zainstalowany szkodliwy kod umożliwia ominięcie zabezpieczeń i zdobycie pełnych uprawnień nad urządzeniem (dostęp do SMS-ów, e-maili, kontaktów, zdjęć itd.). Innym przykładem nowego zagrożenia dla smartfonów jest koń trojański Boxer.AA., który rozsyła wiadomości SMS pod numery

---

[12] http://pclab.pl/news51661.html [dostęp 18.11.2012].

[13] http://mediacenter.avg.com/content/mediacenter/en/news/threat-report-q3-2011.html.

[14] Urządzenie z 2007 roku, mniejsze od iPada.

[15] Wielofunkcyjny komputer typu palmtop z systemem typu Unix i bezprzewodowym dostępem do Internetu; iPod – nazwa rodziny odtwarzaczy multimedialnych firmy Apple.

[16] http://technologie.gazeta.pl/internet/1,104530,12525202,Holenderscy_hakerzy_wykryli_powazna_dziure_w_zabezpieczeniach.html [dostęp 21.09.2012].

o podwyższonej odpłatności. Drogą infekcji są strony WWW udostępniające darmowy dostęp do nielegalnych kopii płatnych gier dla smartfonów z Androidem[17].

Zainfekowane urządzenia można wykorzystywać do kradzieży danych, podsłuchiwania rozmów telefonicznych czy rozsyłania spamu (dzięki możliwości tworzenia botnetów[18]). Z sondażu przeprowadzonego przez AVG Technologies i Ponemon Institute wynika, że na początku 2011 roku ponad jedna trzecia użytkowników smartfonów nie miała świadomości zagrożeń związanych z ich używaniem[19].

Interesujący eksperyment przeprowadziły pod koniec 2011 roku firmy Symantec i Security Perspectives Inc., rozmieszczając 50 smartfonów (zawierających spreparowane informacje osobiste i biznesowe) w publicznych miejscach pięciu miast Ameryki Północnej, a następnie śledząc reakcje ich znalazców[20]. Jedynie połowę urządzeń próbowano zwrócić, w 83% smartfonów uzyskano dostęp do co najmniej jednej aplikacji biznesowej, w 60% przypadków uzyskano dostęp do korespondencji e-mailowej oraz sieci społecznościowych, aż w 43% urządzeń uzyskano dostęp do aplikacji związanej z bankowością online.

4. Mechanizmy i sposoby ochrony rozwiązań mobilnych

Wobec problemów bezpiecznego użytkowania urządzeń mobilnych wymagają one stosowania analogicznych zabezpieczeń jak komputery stacjonarne. Wśród stosowanych sposobów ochrony można wymienić: skanowanie antywirusowe ruchu MMS przez operatorów, preinstalowanie na urządzeniach mechanizmów ochronnych, nieaktywowanie bez potrzeby (i nieakceptowanie nieznanych) połączeń Bluetooth, instalowanie tylko certyfikowanych aplikacji, tworzenie kopii zapasowych systemu operacyjnego i danych, używanie filtru antyspamowego do blokowania niechcianych połączeń telefonicznych i wiadomości tekstowych.

Celem zapewnienia wysokiego poziomu ochrony w urządzenia wbudowuje się różnego rodzaju mechanizmy. Na przykład firma Google wyposażyła system Android (w. 4.0) w obsługę haseł, dzięki czemu aplikacje mogą przechowywać klucze oraz uzyskiwać dostęp do nich i odpowiadających im certyfikatów. Ponadto wprowadzono pełne szyfrowanie urządzenia oraz zestaw narzędzi do obsługi sieci VPN (*Virtual Private Network*)[21] i bezpiecznego przechowywania danych uwierzytelniających. Dodano także funkcję Face Unlock, dzięki której można odblokowywać

---

[17] http://mobtech.interia.pl/systemy-operacyjne/news-zbyt-wysoki-rachunek-za-komorke-moze-zlapales-wirusa,nId,725908 [dostęp 16.12.2012].

[18] Sieci składające się z komputerów, nad którymi zdalnie przejęto kontrolę.

[19] http://news.webwweb.pl/2,44387,0,Uzytkownicy,smartfonow,nieswiadomi,zagrozen.html.

[20] http://enzo.pl/2012/03/22/6-sposobów-na-poprawe-bezpieczenstwa-twojego-smartfona/.

[21] Wirtualna sieć prywatna realizowana w ramach sieci publicznej.

urządzenie na podstawie twarzy właściciela. Z kolei Android 4.2 jest już wyposażony w skaner wirusów.

Opracowywane jest też specjalistyczne oprogramowanie ochronne, takie jak F-Secure Mobile Security czy Kaspersky Mobile Security, przeznaczone między innymi dla systemów Symbian, Windows Mobile i Android. Oprócz podstawowych funkcji zabezpieczających system przed szkodliwymi kodami istotna jest też możliwość zdalnego blokowania lub kasowania danych (na przykład podczas podłączania urządzenia do komputera lub poprzez wysłanie SMS-a) w przypadku zgubienia lub kradzieży urządzenia (np. program Ontrack Eraser Mobile). Inną praktyczną funkcją jest namierzanie sygnału GPS umożliwiające wyświetlenie dokładnej lokalizacji urządzenia (z dokładnością do 1 metra) – w tym celu telefony komórkowe i smartfony są wyposażane w zintegrowane odbiorniki GPS.

W sieciach telefonii komórkowej zapewnia się autentyczność abonentów oraz poufność transmisji głosu i danych, jednak wady stosowanych zabezpieczeń pozwalają je skutecznie atakować. Dla bezpieczeństwa transmisji danych w sieciach GSM stosowany jest szyfr strumieniowy A5. Niestety, w 2008 roku opracowano metodę łamania powszechnie stosowanej wersji A5/1 w czasie krótszym niż pół godziny przy wykorzystaniu dostępnych, niedrogich urządzeń i oprogramowania (zasięg podsłuchu wynosi 20 km). Także mocniejsza wersja szyfru – A5/3, opublikowana w 2007 roku, została trzy lata później złamana[22].

W technologii Wi-Fi dostępnych jest wiele mechanizmów bezpieczeństwa w ramach opracowanych standardów. Z uwagi na słabości WEP i WPA oraz dostępność narzędzi wykorzystujących ich wady do łamania zabezpieczeń zaleca się stosowanie WPA2, wykorzystującego mocniejsze mechanizmy uwierzytelniania oraz zapewnienia integralności i szyfrowania danych.

Podsumowanie

Istotną barierę dla wykorzystywania i dalszego rozwoju mobilnej dostępności zasobów sieciowych może stanowić problem bezpieczeństwa. Użytkownicy rozbudowanych funkcjonalnie urządzeń mobilnych muszą je odpowiednio konfigurować i przestrzegać podstawowych zasad bezpieczeństwa: zabezpieczać urządzenie mocnym hasłem, wyłączać wszystkie nieużywane funkcje, korzystać tylko z pewnych źródeł dystrybucji aplikacji, sprawdzać, jakich pozwoleń żądają aplikacje podczas ich instalacji, i używać odpowiedniego systemu chroniącego dane.

Niestety, przewiduje się dalszy dynamiczny wzrost zagrożeń dla urządzeń mobilnych, dlatego należy opracować nowe, bardziej skuteczne rozwiązania w zakresie ich ochrony.

---

[22] www.securitystandard.pl/news/354691/Atak.na.szyfr.komorek.3G.html.

Literatura

1. http://enzo.pl/2012/03/22/6-sposobow-na-poprawe-bezpieczenstwa-twojego-smartfona/ [22.03.2012].
2. http://ey.media.pl/pr/226896/uzytkownicy-smarfonow-nie-wykorzystuja-ich-potencjalu-boja-sie-wyzszych-rachunkow [7.11.2012].
3. http://mediacenter.avg.com/content/mediacenter/en/news/threat-report-q3-2011.html.
4. http://news.webwweb.pl/2,44387,0,Uzytkownicy,smartfonow,nieswiadomi,zagrozen.html.
5. http://pclab.pl/news51648.html [16.11.2012].
6. http://pclab.pl/news51661.html [18.11.2012].
7. http://tech.wp.pl/kat,1009781,title,Zbyt-wysoki-rachunek-za-komorke-moze-zlapales-wirusa [13.12.2012].
8. Kędzierski R.: *Holenderscy hakerzy wykryli poważną dziurę w zabezpieczeniach iPhone'a 4S i 5*, http://technologie.gazeta.pl/internet/1,104530,12525 202, Holenderscy_hakerzy_wykryli_powazna_dziure_w_zabezpieczeniach.html [21.09.2012].
9. Kutera T.: *Jak Polacy łączą się z siecią?* [24.11.2011].
10. Sosnowska J.: *Historia zatoczyła koło – triumfalny powrót tabletów PC*, http://technologie.gazeta.pl/internet/1,113841,12828126,Historia_zatoczyla_kolo__triumfalny_powrot_tabletow.html [9.11.2012],
11. www.orange.pl/ocp-http/PL/Binary2/1979463/4053940725.pdf
12. www.securitystandard.pl/news/354691/Atak.na.szyfr.komorek.3G.html.

THE AVAILABILITY OF INTERNET RESOURCES WITH THE USE OF MOBILE DEVICES

Summary

The usage of mobile devices accessing internet resources is getting more and more common. Easy to operate and rich in functions, these devices are used for communication, accessing a variety of services and realization of business tasks. Unfortunately, for about past two years a dynamic increase in the number of security threats has been observed which may pose an obstacle in secure use of such devices and impose further development of hardware and software security mechanisms.

Translated by Zygmunt Mazur