Nierówności Społeczne a Wzrost Gospodarczy, nr 44 (4/2015), część 2
DOI: 10.15584/nsawg.2015.4.2.2 **ISSN 1898-5084**

dr inż. Teresa Mendyk-Krajewska[1]
dr hab. Zygmunt Mazur[2]
mgr Hanna Mazur[3]
Instytut Informatyki, Wydział Informatyki i Zarządzania
Politechnika Wrocławska

Mobilna dostępność Internetu w społeczeństwie informacyjnym – rozwój i zagrożenia

WPROWADZENIE

Powszechny dostęp do systemów i sieci komputerowych stworzył podstawę rozwoju społeczeństwa informacyjnego. Systemy teleinformatyczne umożliwiają gromadzenie i przetwarzanie danych, szybkie komunikowanie się i realizację usług. Urządzenia mobilne[4], dzięki nieustannie rozwijanym technologiom transmisji bezprzewodowej, stanowią dużą konkurencję dla konwencjonalnych komputerów PC, umożliwiając szybki dostęp do Internetu z dowolnego miejsca i podczas przemieszczania się. Liczne zalety mobilnego dostępu do sieci komputerowych spowodowały duże zainteresowanie nowymi technologiami, wymuszając ich dynamiczny rozwój obserwowany w ostatnich latach.

Wszelkie działania prowadzone za pomocą rozwiązań mobilnych muszą być niezawodne i bezpieczne. By mogły być powszechnie stosowane i rozwijane, coraz większą wagę przywiązuje się zarówno do poprawy parametrów transmisji danych i wzrostu funkcjonalności urządzeń, jak i do zapewnienia wysokiego poziomu ochrony systemów. Urządzenia mobilne często wykorzystywane są do

[1] Adres korespondencyjny: Instytut Informatyki, Wydział Informatyki i Zarządzania, Politechnika Wrocławska, Wyb. Wyspiańskiego 27, 50-370 Wrocław, e-mail: teresa.mendyk-krajewska@pwr.edu.pl, tel. 71 320 39 69.
[2] Adres korespondencyjny: Instytut Informatyki, Wydział Informatyki i Zarządzania, Politechnika Wrocławska, Wyb. Wyspiańskiego 27, 50-370 Wrocław, e-mail: zygmunt.mazur@pwr.edu.pl, tel. 71 320 42 23.
[3] Adres korespondencyjny: Instytut Informatyki, Wydział Informatyki i Zarządzania, Politechnika Wrocławska, Wyb. Wyspiańskiego 27, 50-370 Wrocław, e-mail: hanna.mazur@pwr.edu.pl, tel. 71 320 42 23.
[4] Przenośne urządzenia elektroniczne, np. laptop, smartfon, tablet czy fablet, umożliwiające przetwarzanie i bezprzewodowe przesyłanie danych.

przechowywania i przesyłania danych poufnych, co potwierdzają zamieszczone wyniki przeprowadzonej ankiety dotyczącej ich użytkowania. Celem publikacji jest ukazanie dynamiki rozwoju mobilnej dostępności Internetu oraz podkreślenie znaczenia bezpieczeństwa dla szerokiego wykorzystania rozwiązań bezprzewodowych.

KIERUNKI ROZWOJU TECHNOLOGII BEZPRZEWODOWYCH

Na dynamiczny rozwój technologii bezprzewodowych wpływają ich zalety, w tym możliwości ich szerokiego zastosowania. Dla poprawy jakości świadczonych usług, ze względu na konieczność zapewnienia współpracy między dostępnymi standardami, potrzebę zwiększenia prędkości transmisji i efektywniejszego wykorzystania łączy – wszystkie technologie transmisji bezprzewodowej (Wi-Fi, telefonii komórkowej i transmisji satelitarnej) są systematycznie rozwijane. Nieustannie opracowywane są nowe standardy.

Współczesne systemy transmisji satelitarnej to VSAT *(Very Small Aperture Terminal*) – system łączności wykorzystujący satelity geostacjonarne, używany w terenie pozbawionym naziemnej infrastruktury, skupiający różne standardy przeznaczone m.in. do zapewnienia dostępności Internetu, transmisji wideo i połączeń głosowych oraz Iridium – system wykorzystujący satelity na niskich orbitach[5], z którego m.in. korzystają wojsko, organizacje rządowe i żegluga.

Z powodu potrzeby wzrostu prędkości przesyłu łączami satelitarnymi, w coraz większym stopniu będzie wykorzystywane pasmo Ka (o wyższej częstotliwości niż używane pasma C i Ku[6]), wymagające stosowania skomplikowanych systemów satelitarnych z powodu mniejszej odporności na zakłócenia [Silverstein, 2013]. Przewiduje się, że m.in. poprawę jakości transmisji można będzie osiągnąć dzięki większym zasobom energii elektrycznej przy wykorzystaniu baterii słonecznych [Amyotte, Camelo, 2011]. Z kolei odpowiednie systemy mechaniczne i elektroniczne umożliwiające konfigurowanie satelitów po ich umieszczeniu na orbicie pozwolą zwiększyć czas eksploatacji satelitów i elastyczność całego systemu. Prowadzone są prace nad standardem Iridium NEXT. Przewidywana prędkość transmisji danych do urządzeń mobilnych wynosi 1,5 Mb/s, zaś do stałych i ruchomych terminali wyposażonych w anteny satelitarne – 8 Mb/s. Wykorzystywana szerokość pasma ma być znacznie zwiększona, a jego alokacja bardziej elastyczna. Istnieją plany stopniowej wymiany wszystkich satelitów w latach 2015–2017.

[5] Umieszczone ok. 780 km n.p.m. na 6 płaszczyznach orbitalnych, obejmują swoim zasięgiem całą Ziemię.

[6] Pasma wykorzystywane głównie w transmisji telewizji satelitarnej analogowej, cyfrowej i HDTV, a także do satelitarnych połączeń internetowych.

Równie dynamicznie rozwijane są technologie transmisji telefonii komórkowej. Wykorzystywane dotąd standardy (GSM[7], UMTS[8], HSPA[9]) ma zastąpić nowa technologia LTE-Advanced[10], której wdrożenia planowane są na lata 2015–2016. Wśród wymagań dla sieci komórkowych czwartej generacji (4G) [4G, 2013] zdefiniowanych przez organizację ITU (*International Telecommunication Union*) wyróżnić można następujące [4G, 2012]:

- sieć działa z wykorzystaniem komutacji pakietów i protokołem IP,
- współdziała z istniejącymi standardami sieci bezprzewodowych,
- skalowalna szerokość kanału wynosi 5–20 MHz, opcjonalnie do 40 MHz,
- nominalna prędkość transmisji to 100 Mb/s, gdy urządzenie porusza się z dużą prędkością względem stacji nadawczo-odbiorczej i 1 Gb/s, gdy urządzenie i stacja są wobec siebie we względnie stałym położeniu[11],
- zdolność do zapewnienia wysokiej jakości usług multimedialnych,
- dynamiczne dzielenie się zasobami sieci i ich użytkowanie dla jednoczesnego wspierania większej liczby użytkowników w obrębie komórki (obszaru kontrolowanego przez stację bazową).

Testowany obecnie standard bezprzewodowego przesyłu danych LTE-Advanced zapewnia większą efektywność widmową, wprowadza większe prędkości przesyłu (do stacji bazowej i ze stacji bazowej, zarówno w dostępie statycznym jak i mobilnym). Posiada również funkcję koordynacji sieci oraz agregację częstotliwości nośnych, a także szereg usprawnień. Jednym z nowych rozwiązań jest możliwość rozszerzania sieci z wykorzystaniem komórek przekaźniczych zamiast pełnego wdrażania stacji bazowej (mniejsze nakłady finansowe). Dla odciążenia sieci opracowano też protokół Home eNode B[12], dzięki któremu transfer wymagający dużych zasobów (np. ruchomego obrazu) może być przekazany przez sieci Wi-Fi. W kolejnych wydaniach specyfikacji LTE-Advanced wprowadzono techniki zwiększające wydajność systemu i usprawnienia dla samodzielnej optymalizacji sieci, dodano protokoły do przesyłania informacji dotyczących jakości transmisji oraz nowe mechanizmy oszczędzania energii kosztem jakości usługi, zasięgu i pojemności. W 12 wydaniu LTE-Advanced (zakończenie prac ma nastąpić w 2014 r.) nacisk kładzie się na tzw. zagęszczanie sieci, polegające na zwiększaniu liczby węzłów przekaźnikowych o małej mocy (nie muszą cechować

[7] *Global System for Mobile Communications* – najbardziej rozpowszechniony standard telefonii komórkowej.

[8] *Universal Mobile Telecommunications System* – system trzeciej generacji (3G).

[9] *High Speed Packet Access* – 3,5G.

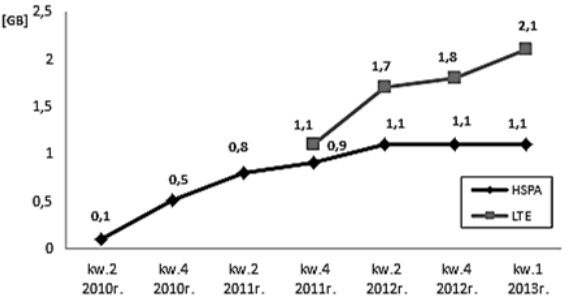
[10] Zalicza się tu LTE (*Long Term Evolution*) od 10 wersji specyfikacji sfinalizowanej w 2013 roku, standard LTE opracowany został przez konsorcjum 3GPP (*3 Generation Partnership Project*), wszystkie jego późniejsze wydania oparte są na 8 wersji specyfikacji z 2008 r.

[11] Do systemów 4G mogą być zaliczane też te nie osiągające prędkości 1 Gb/s przy małej mobilności, jeśli są dużo wydajniejsze niż 3G i rokują osiągnięcie tego wymogu w przyszłości.

[12] Home enhanced Node B – rodzaj nadajnika telefonii komórkowej zapewniającego użytkownikowi dostęp do usługi sieci 4G; łączy się z siecią operatora przy pomocy Internetu.

się bardzo dużą niezawodnością i zasięgiem) pozostających w zasięgu stacji bazowej. Efektem jest zwiększenie pojemności sieci przy mniejszym obciążeniu pojedynczych węzłów i ich niższym poborze mocy.

Ponadto opracowywane są rozwiązania dla pracy węzłów z częstotliwością różną od wykorzystywanej przez stację bazową. Wydanie to wprowadza też dalsze usprawnienia prowadzące do zwiększenia zasięgu komórki. Rozwój technologii obejmuje również możliwość wzajemnego wykrywania się i komunikację między znajdującymi się w pobliżu urządzeniami klienckimi. Technologia LTE szybko wypiera wcześniej stosowaną HSPA i przewiduje się jej dalszy rozwój. W marcu 2013 r. LTE udostępniało 151 komercyjnych sieci w 67 krajach, natomiast w sierpniu 2013 r. aż 200 sieci w 76 krajach. Polska jest pierwszym krajem europejskim, w którym wdrożono Internet LTE w paśmie 1800 MHz z prędkością do 150 Mb/s (Plus i Cyfrowy Polsat) [Świderski, 2013]. Porównanie średniej ilości pobieranych danych w ciągu miesiąca w obu sieciach zestawiono na rys. 1.



Rysunek 1. Średnia ilość pobieranych danych w wybranych kwartałach lat 2010–2013

Źródło: opracowanie własne na podstawie [Fitchard, 2014].

Wynikiem prac nad rozwojem bezprzewodowych sieci komputerowych WLAN (technologia Wi-Fi) jest powstanie standardu 802.11ac jako uzupełnienia standardu 802.11n. Zdefiniowano w nim pasmo transmisyjne o częstotliwości 5 GHz wykorzystujące kanały o szerokości 20, 40 i 80 MHz[13], co daje dwukrotnie większą przepustowość[14] niż w standardzie 802.11n. Dzięki zastosowaniu modulacji 256 QAM (*Quadrature Amplitude Modulation*) oraz zwiększeniu liczby anten w technologii MIMO[15], osiągnięto wzrost przepustowości i zasięgu. Uzyskano

[13] Składa się z dwóch sąsiadujących kanałów 40 MHz.

[14] Przewiduje się możliwość wykorzystania kanałów 160 MHz, które będą się składały z sąsiadujących i niesąsiadujących kanałów o szerokości 80 MHz.

[15] Technologia MIMO niweluje negatywną interferencję sygnałów, co zwiększa niezawodność transmisji; stosowana w bezprzewodowych sieciach komputerowych, telefonii komórkowej i telewizji cyfrowej.

też poprawę efektywności transmisji przez zastosowanie mechanizmu dynamicznego zarządzania pasmem [IEEE802…, 2012].

Wykorzystanie zalet technologii 802.11ac wymaga modernizacji infrastruktury i wymiany urządzeń. Technologia Wi-Fi jest też dostępna w smartfonach. Szacuje się, że w 2015 roku smartfony pracujące zgodnie ze standardem 802.11ac będą powszechnie stosowane i będzie ich ok. 1 mld [*Zero to a Billion…*]. W tym celu producenci instalują w urządzeniach odpowiednie chipy radiowe, np. firma Apple wyposażyła w nie notebooki MacBook Air, zaś inne firmy zainstalowały je w swoich telefonach: HTC w HTC One, a Samsung w Galaxy S4.

Firma Huawei testuje standard 802.11ax, dopuszczający jeszcze większe prędkości (w paśmie 5 GHz prędkość może być 10-krotnie większa niż w 802.11 ac) i według jej przewidywań w 2018 roku będzie on powszechnie stosowany [Jackson, 2014]. Wszystkie wprowadzone rozwiązania wynikają z konieczności usprawnienia łączności bezprzewodowej wobec gwałtownego wzrostu liczby użytkowników urządzeń mobilnych z dostępnością sieci Internet, wraz z rozwojem realizowanych z jej wykorzystaniem usług.

MOBILNY DOSTĘP DO INTERNETU

Od kilkunastu lat obserwuje się dynamiczny rozwój urządzeń mobilnych. Wygoda ich użytkowania, coraz lepsze dostosowanie do potrzeb użytkownika i rosnąca funkcjonalność, przy coraz niższych kosztach zakupu i eksploatacji sprawiają, że urządzenia te są niemal powszechnie używane. Oferują użytkownikom dostęp do Internetu (w tym do poczty elektronicznej i portali społecznościowych), służą do realizacji zadań biznesowych (umożliwiając stały dostęp do zasobów firmy), pozwalają na wygodne korzystanie z wszelkiego rodzaju usług.

Gwałtowny wzrost sprzedaży urządzeń mobilnych nastąpił w 2010 r. i wynikał z przejęcia przez nowo wprowadzane modele smartfonów i tabletów funkcji komputerów PC. W okresie X–XII 2012 r. na świecie sprzedaż tabletów wzrosła o 75% w stosunku do IV kw. 2011 r. i wyniosła 52,5 mln [Kreft, 2013], a w 2013 r. sprzedano o 50% więcej tabletów niż w 2012 r. [*Krzepnie…*, 2014]. Tendencja wzrostowa dotyczy również smartfonów – w I kw. 2014 r. sprzedano ich ok. 30% więcej niż w I kw. 2013 r. [Domański, 2014]. Bezkonkurencyjnym liderem na rynku oprogramowania urządzeń mobilnych stał się Android (od 2004 r. właścicielem jest Google) stanowiący platformę programową obejmującą system operacyjny, warstwę pośrednią i najważniejsze aplikacje [Collins i in., 2012]. Wysoką pozycję zapewnia mu otwarta licencja, dobrze opracowane i udokumentowane API[16] (umożliwiające łatwe tworzenie aplikacji) oraz niezależność sprzętowa. Architekturę Androida tworzą cztery warstwy:

[16] *Application Programming Interface*, zbiór zasad komunikowania się między sobą oprogramowania komputerowego.

- jądro systemu (*Linux Kernel Layer*) – odpowiedzialne za zarządzanie procesami i pamięcią, bezpieczeństwo, sterowniki sprzętowe oraz zasilanie,
- natywne biblioteki sytemu (*Native Libraries Layer*) – zbiór bibliotek używanych przez komponenty systemu (m.in. silnik przeglądarki internetowej, do obsługi baz danych SQL i odbiornika GPS, komunikacji z innymi urządzeniami czy wyświetlania grafiki); na tym poziomie znajduje się też warstwa wykonawcza (Android Runtime Layer),
- framework do tworzenia aplikacji (*Applications Framework Layer*),
- warstwa aplikacji składających się na funkcjonalność urządzenia.

Daleko za Androidem (80%), na drugim miejscu w rankingu popularności, znalazł się system operacyjny firmy Apple – iOS (12%) [Kędzierski, 2013]. Pozostałe dostępne na rynku oprogramowanie, jak np. Phone i Mobile firmy Microsoft czy tak popularny niegdyś Symbian, nie cieszą się zainteresowaniem użytkowników i ich sprzedaż nie przekracza 5%.

Według badań przeprowadzonych przez firmę Google w 2013 roku – 39% posiadaczy smartfonów korzysta z nich codziennie. Oprócz wykorzystywania podstawowych funkcji telefonu użytkownicy najczęściej przeglądają Internet (poszukują informacji, słuchają muzyki, grają w gry komputerowe itp. – 91%), sięgają do poczty elektronicznej i sieci społecznościowych (82%) oraz przeglądają określone treści (blogi, serwisy ogłoszeniowe itp. – 73%) [think].

W 2013 r. 14% ruchu w Internecie pochodziło z urządzeń mobilnych (w 2011 r. – 8,5% [*Już…*, 2014], a w 2010 – zaledwie 3% [Kreft, 2013]). Analitycy z firmy Cisco przewidują, że już w 2018 r. większość ruchu będą generować urządzenia mobilne [Jaślan, 2014]. W Polsce w 2013 r. do sieci było podłączonych 99,6 mln urządzeń, przy czym zdecydowany udział miały komputery stacjonarne (83% ruchu). Według prognoz do 2018 r. średnia przepustowość łącza szerokopasmowego w Polsce wzrośnie do 37Mb/s – będzie to 2,5-krotny wzrost w stosunku do roku 2013 (15,1 Mb/s).

Z systematycznie prowadzonych analiz firmy Ericson wynika, że obecnie na świecie jest 6,9 mld subskrypcji dla urządzeń mobilnych (w 2011 r.: 5,9 mld, w 2012 r.: 6,2 mld, w 2013 r.: 6,7 mld) [*Global…*, 2014]. Firma szacuje, że w 2019 roku liczba mobilnych urządzeń sięgnie aż 9,3 mld, a liczba smartfonów będzie na poziomie 765 mln. Urządzenia te są obecnie bardzo zaawansowane technicznie. Nowe wersje wnoszą usprawnienia w wydajności i kompatybilności pomiędzy dostępnymi standardami, a także poprawę poziomu ochrony, gdyż ze wzrostem funkcjonalności urządzeń i rozwojem usług pojawiają nowe zagrożenia dla ich bezpiecznego użytkowania. Podstawę bezpieczeństwa stanowi fizyczna ochrona urządzeń oraz kontrola dostępu do systemu, jednak wobec realnych zagrożeń, w kolejnych wersjach urządzeń pojawiają się coraz doskonalsze mechanizmy zabezpieczeń, które obejmują dane, ruch sieciowy i zainstalowane oprogramowanie. Do aktywacji urządzenia coraz częściej wykorzystuje się technologie biometryczne. Przykładami mogą być funkcja Face Unlock w najnowszych

wersjach systemu Android umożliwiająca analizę twarzy użytkownika oraz czytnik linii papilarnych Touch ID w urządzeniach iPhone firmy Apple i w Galaxy S5 firmy Samsung. Dla bezpieczeństwa wprowadza się też wiele rozwiązań programowych. Jednym z nich jest blokada niepożądanych usług, tj. bezprawnego wysyłania wiadomości czy programów pobieranych spoza oficjalnych źródeł. Specjalne systemy (np. Google Bouncer) skanują aplikacje Google Play pod kątem szkodliwych kodów, a w nowszych wersjach Androida działanie to poszerzono o monitorowanie zainstalowanych aplikacji pochodzących z nieoficjalnych źródeł (system Verify apps) [Hellman, 2014]. Dla bezpieczeństwa ogranicza się też prawa aplikacjom (kontrolując ich dostęp do danych), losowo przydziela adresy pamięci (aby utrudnić szkodliwym kodom lokalizację elementów systemu), izoluje programy (by aplikacje miały dostęp jedynie do wcześniej przydzielonych zasobów), a także wprowadza szyfrowanie pamięci wewnętrznej urządzenia.

Firma Apple w swoich urządzeniach także oferuje zabezpieczenia w celu blokady instalacji niebezpiecznych aplikacji, działania szkodliwych funkcji i nieuprawnionego dostępu do danych. Umożliwia również ich szyfrowanie, a deszyfrowanie następuje po poprawnej autoryzacji użytkownika, zaś aplikacje posiadają podpis lub certyfikat firmy Apple. Mnogość instalowanych zabezpieczeń w urządzeniach mobilnych wskazuje na wagę problemu. Niestety, mimo coraz lepszych sposobów ochrony urządzenia te nie są całkowicie bezpieczne.

ZAGROŻENIA DLA URZĄDZEŃ MOBILNYCH

Równolegle z rosnącą popularnością urządzeń mobilnych i ilością przechowywanych na nich danych, obserwuje się wzrost zagrożeń dla ich bezpiecznego użytkowania. Systemom mobilnym zagraża szkodliwe oprogramowanie (wirusy, konie trojańskie, programy umożliwiające podsłuch itp.) oraz możliwość bezprawnego użycia urządzenia. Celem ataków na systemy są nazwy i hasła dostępowe do kont pocztowych, portali społecznościowych lub stron WWW, a także przechowywane listy kontaktów, treści SMS-ów czy zdjęcia. Od czasu udostępnienia w urządzeniach mobilnych funkcji płatności (coraz więcej smartfonów wykorzystuje też technologię NFC do płatności zbliżeniowych) przedmiotem zainteresowania przestępców stały się także dane związane z użytkowaniem kont bankowych oraz kart płatniczych i kredytowych.

Zidentyfikowano tysiące sygnatur szkodliwych kodów dla urządzeń mobilnych, które wykonują szereg niepożądanych działań, takich jak: blokowanie karty pamięci lub całego urządzenia, uszkadzanie, usuwanie lub nielegalne pozyskiwanie danych, zdalne udostępnianie urządzenia, śledzenie jego lokalizacji, czy wyłączanie mechanizmów bezpieczeństwa systemu. Szczególny rodzaj zagrożenia stwarzają kody serwisowe (pomagające diagnozować problemy i zmieniać parametry konfiguracyjne urządzenia), jeśli zostaną np. zdalnie zainstalowane i użyte

przez osoby nieuprawnione. Dodatkowym problemem jest możliwość wykorzystania zainfekowanego urządzenia do bezprawnego wykonywania połączeń, wysyłania spamu lub przeprowadzenia ataku.

Obserwowany wzrost zagrożeń dla urządzeń mobilnych cechuje znacznie większe tempo niż w przypadku tradycyjnych komputerów PC. Szkodliwe programy potrafią rozprzestrzeniać się przy pomocy przenośnych nośników pamięci, komunikatów MMS i SMS, czy z wykorzystaniem technologii Bluetooth. Jedną z istotnych dróg infekcji systemu mobilnego stanowi zdalne pobieranie plików (tj. dzwonków, grafiki, gier i oprogramowania użytkowego). Aplikacje mogą nieść zagrożenie, nawet gdy pochodzą z oficjalnych źródeł, takich jak Google Play czy App Store. Na przykład w maju 2014 r. w firmowym sklepie Googla zidentyfikowano aplikację KK Tuneup Master, której główną funkcją jest poprawa wydajności urządzenia, lecz wywołuje też wiele niepożądanych działań, takich jak wysyłanie wiadomości pod numery usług o wysokiej opłacie czy instalowanie innych aplikacji bez wiedzy użytkownika [*Uwaga…*, 2014]. Do przeprowadzenia ataku można wykorzystać przeglądarkę internetową [Gliwiński, 2012]. Dużym zagrożeniem dla bezpieczeństwa jest także niezabezpieczona sieć bezprzewodowa [Fry…, 2010].

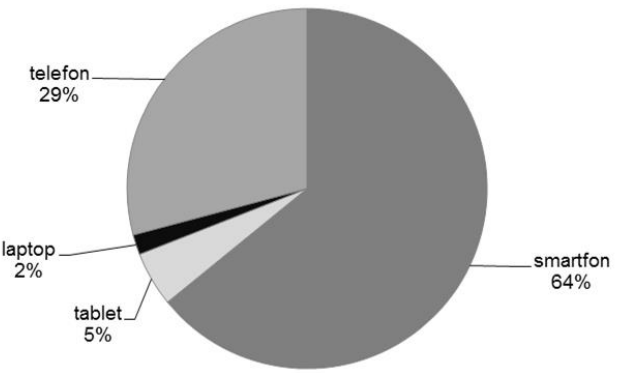
Problem z utrzymaniem bezpieczeństwa urządzeń mobilnych wynika również z braku posiadania przez użytkowników najnowszych zaktualizowanych wersji oprogramowania. Według statystyk, aż 77% zagrożeń można byłoby wyeliminować, gdyby wszystkie urządzenia z systemem Android zawierały jego zaktualizowane wersje [*Third…*, 2013].

Dotyczy to też oprogramowania innych firm, nie tylko Google. Tak samo bowiem jak dla systemów konwencjonalnych, dla rozwiązań mobilnych opracowywane są narzędzia wykorzystujące wady oprogramowania w celu uzyskania nieupoważnionego dostępu do urządzenia. W konsekwencji może ono stać się częścią sieci tworzonej z przejętych urządzeń mobilnych (tzw. botnetu), które wykorzystywane są do prowadzenia bezprawnych działań.

Przeważająca większość ataków na systemy mobilne wymierzona jest w system Android z powodu popularności tej platformy i jej otwartości (każdy może mieć dostęp do architektury i kodu źródłowego). Spośród 277 zagrożeń zidentyfikowanych w I kw. 2014 roku, aż 275 wymierzonych było właśnie w oprogramowanie Android firmy Google, a tylko po jednym na iPhone i Symbian [*Mobile…*, 2014]. Większość zagrożeń stanowiło szkodliwe oprogramowanie, a w szczególności konie trojańskie (88%, np. Backdoor.AndroidOS.Obad.a czy FakeSite.A (Perkele)). Działanie szkodliwych aplikacji ma być dla użytkownika niezauważalne, a do ich tworzenia można wykorzystać gotowe zestawy narzędzi (malware tool kits). Z testów przeprowadzonych przez redakcję czasopisma „Chip" wynika, że wzrasta zainteresowanie atakami na system Android [Malinowski, 2013].

System iOS pod względem bezpieczeństwa różni się od Androida [Zdziarski, 2013]. Jest to system zamknięty (zatem trudny do penetracji), a kontakt z siecią jest ograniczony, co utrudnia zdalny dostęp do urządzenia. Zagrożenie stwarza tzw. jailbreaking – usunięcie ograniczeń wprowadzonych przez firmę Apple (przy użyciu darmowych narzędzi dostępnych w Internecie), umożliwiające uzyskanie nad systemem pełnej kontroli, ale także przeprowadzenie ataku. Brak zaufania do bezpieczeństwa oferowanych systemów mobilnych powoduje, że np. w Chinach prowadzone są prace nad własnym systemem operacyjnym. W sierpniu 2014 roku rząd chiński podjął decyzję o zakazie zakupu z pieniędzy publicznych urządzeń firmy Apple (z obawy o możliwość szpiegowania) [Gałuszka, 2014].

Odrębny problem stanowi możliwość lokalizacji urządzenia mobilnego. Bezpieczne korzystanie ze smartfona wymaga odpowiedniej konfiguracji (szczególnie dotyczy to systemu Android), bowiem po zainstalowaniu określonych aplikacji, możliwe jest śledzenie użytkownika. Fakt ten podkreślił John McAfee w sierpniu 2014 roku na konferencji Def Con w Las Vegas [Yadron, 2014]. Wszelkie naruszenia w tym zakresie można zgłaszać na utworzonej przez niego stronie internetowej brownlist.com.



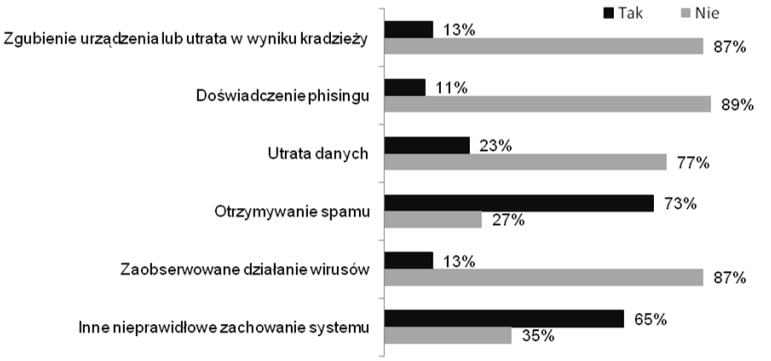
Rysunek 2. Sprzęt wykorzystywany przez ankietowanych do realizacji e-usług

Źródło: opracowanie własne na podstawie wyników ankiety.

Z ankiety przeprowadzonej przez autorów w maju 2014 r. wśród 221 studentów II i III roku kierunku informatyka wynikało, że prawie 25% z nich wykorzystuje urządzenia mobilne do przechowywania poufnych danych, a prawie połowa (47%) wykorzystuje te urządzenia do przekazywania takich danych, pomimo, że mają świadomość istnienia realnych zagrożeń (ponad 91%). Większość urządzeń mobilnych będących w posiadaniu ankietowanych to smartfony. Na rys. 2 przedstawiono procentowe zestawienie wykorzystywanych rodzajów urządzeń mobilnych.

Chociaż zdecydowana większość użytkowników zdawała sobie sprawę z istnienia problemu bezpieczeństwa, niewiele robi dla jego poprawy. Niespełna 30% ankietowanych miało zainstalowane oprogramowanie ochronne, w wielu przypadkach był to jedynie komponent oprogramowania systemowego. Zdaniem części ankietowanych dodatkowe oprogramowanie dla systemów iOS i Android było zbędne. Podobnego zdania o swoich produktach jest firma Google [Tkacz, 2014]. Niestety, mimo firmowego zabezpieczenia wielu użytkowników systemu Android doświadczyło ataków.

Wśród osób uczestniczących w badaniu ponad 65% zaobserwowało nieprawidłowe działanie systemu, a ponad 73% otrzymywało spam. Wyniki dotyczące rodzajów rejestrowanych przez nich zagrożeń zostały pokazane na rys. 3.



Rysunek 3. Odsetek osób, które doświadczyły wybranych zdarzeń na użytkowanym urządzeniu

Źródło: opracowanie własne na podstawie wyników ankiet.

PODSUMOWANIE

Coraz powszechniejsze wykorzystywanie rozwiązań bezprzewodowych, z racji rozlicznych zalet, wymusza opracowywanie nowych standardów technologicznych i sprzętowych celem poprawy jakości świadczonych usług. Wraz ze wzrostem popularności urządzeń mobilnych i intensywnym rozwojem ich funkcjonalności (w szczególności dostępności Internetu) – rośnie liczba zagrożeń dla bezpiecznego ich użytkowania. Mobilne systemy operacyjne wykazują szereg podatności, które mogą być wykorzystywane do przeprowadzania ataków, dlatego niezależnie od firmowych zabezpieczeń dla wyższego poziomu ochrony można zainstalować dodatkowe oprogramowanie, które obok podstawowych funkcji (skanowanie, filtrowanie, kontrola praw dostępu, monitorowanie) umożliwi tworzenie kopii zapasowych i zabezpieczy sprzęt na wypadek kradzieży (pozwoli zlokalizować urządzenie, a w razie potrzeby umożliwi zablokowanie dostępności lub usu-

nięcie danych. Problemu bezpieczeństwa nie należy bagatelizować, gdyż niedostateczna ochrona rozwiązań mobilnych może stanowić barierę dla ich dalszego rozwoju. Na skutek infekcji systemu można ponieść straty finansowe, utracić dane, ponosić koszty związane z ich odzyskaniem, naprawą urządzenia, wymianą elementów lub całego urządzenia, a nawet odpowiadać za nadużycia dokonane z zainfekowanego sprzętu.

BIBLIOGRAFIA

4G – A Small Introduction, vendorupsc.jeywin.com/main/4g-a-small-introduction, 2012.

4G Americas, *3GPP Release 11: Understanding the Standards for HSPA+ and LTE-Advanced Enhancements*, 4G Americas, 2013.

Amyotte E., Camelo L., 2011, *TechTalk: Future Trends: Satellite Communication Antennas*, satmagazine.com/story.php?number=1928571183.

androidnius.pl/10-zasad-bezpiecznego-korzystania-ze-smartfonow-i-tabletow, 2014.

Collins Ch., Galpin M., Kaeppler M., 2012, *Android w praktyce*, Helion, Gliwice.

Domański T., *Samsung zdominował rynek smartfonów*, „Chip", 2014, www.chip.pl/news/sprzet/telefony/2014/05/samsung-zdominowal-rynek-smartfonow.

Fitchard K., 2014, *Report: As countries adopt LTE, mobile data use starts skyrocketing, gigaom.com/2014/01/20/report-as-countries-adopt-lte-mobile*-data-use-starts-skyrocketing.

Fry C., Nystrom M., 2010, *Monitoring i bezpieczeństwo sieci*, Helion, Gliwice.

Gałuszka D., 2014, *Nie dla sprzętu Apple w Chinach*, mobiletrends.pl.

Gliwiński M., 2012, *Ataki na strony internetowe*, Wydawnictwo CSH, Kwidzyn.

Global mobile statistics 2014 Part A: Mobile subscribers; handset market share; mobile operators, 2014, mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers.

Hellman E., 2014, *Platforma Android. Nowe wyzwania*, Helion, Gliwice.

IEEE802.11ac: The Next Evolution of Wi-Fi™ Standards, QUALCOMM Incorporated, 2012, qualcomm.com/media/documents/files/ieee802-11ac-the-next-evolution-of-wi-fi.pdf.

Jackson M., 2014, *Next Generation 10Gbps WiFi at 5GHz Successfully Tested and Due in 2018*, ispreview.co.uk/index.php/2014/05/next-generation-10gbps-wifi-5ghz-successfully-tested-due-2018.html.

Jaślan M., 2014, Cisco: *W 2018 roku większość ruchu IP będą generować urządzenia mobilne*, polskaszerokopasmowa.pl/artykuly/cisco-w-2018-roku-wiekszosc-ruchu-ip-beda-generowac-urzadzenia-mobilne.html.

Już 8,5% ruchu w Internecie generują urządzenia mobilne, 2014, http://m.technologie.gazeta.pl/internet/55,113033,11100711,,,,11100631.html.

Kędzierski R., 2013, *80% smartfonów działa pod kontrolą jednego systemu operacyjnego*, technologie.gazeta.pl/internet/1,104530,14405708,80__smartfonow_dziala_pod_kontrola_ jednego_systemu.html.

Kreft P., 2013, *Urządzenia mobilne generują coraz więcej ruchu w sieci*, „Komputer Świat".

Krzepnie rynek tabletów, „Rzeczpospolita", 2014, www.ekonomia.rp.pl/artykul/1083937.html.

Malinowski J., 2013, *Wielkie porównanie antywirusów dla Androida*, „Chip".

Mobile Threat Report Q1 2014, F-Secure Labs 2014.

Silverstein S., 2013, *Antenna Industry: Tuned to Future of Satellite Communications*, Via Satellite, satellitetoday.com/publications/via-satellite-magazine/features/2013/02/01/antenna-industry-tuned-to-future-of-satellite-communications.

Świderski B., 2013, *LTE w Polsce i na świecie. Ile państw z tego korzysta i jak Polska wypada na ich tle*, http://natemat.pl/74037,lte-w-polsce-i-na-swiecie-ile-panstw-z-tego-korzysta-i-jak-polska-wypada-na-ich-tle.

think.withgoogle.com/mobileplanet/pl.

Third Annual Mobile Threats Report: March 2012 through March 2013, 2013, Juniper Networks Mobile Threat Center.

Tkacz Ł., 2014, *Google: antywirus na Androidzie nie jest do niczego potrzebny*, www.dobreprogramy.pl/Google-antywirus-na-Androidzie-nie-jest-do-niczego-potrzebny,News,56239.html.

Uwaga na groźną aplikację w sklepie Google Play, 2014, www.pclab.pl/pr58027.html.

Yadron D., 2014, *John McAfee at Def Con: Don't use smartphones*.

Zdziarski J., 2013, *Łamanie i zabezpieczanie aplikacji w systemie iOS*, Helion, Gliwice.

Zero to a Billion; 802.11ac-Enabled Device Shipments to Soar by 2015, Says In-Stat, 2011, www.marketwired.com/press-release/zero-to-a-billion-80211ac-enabled-device-shipments-to-soar-by-2015-says-in-stat-1391854.htm.

Streszczenie

Liczne zalety mobilnego dostępu do Internetu spowodowały duże zainteresowanie rozwiązaniami bezprzewodowymi wpływając na ich dynamiczny rozwój obserwowany w ostatnich latach. Możliwości i coraz powszechniejsze wykorzystanie urządzeń mobilnych wymuszają opracowywanie nowych standardów transmisji bezprzewodowej w celu poprawy jakości usług. Wszystkie technologie są systematycznie rozwijane ze względu na konieczność zapewnienia między nimi współpracy, potrzebę wzrostu prędkości transmisji i efektywniejszego wykorzystania łączy.

Działania prowadzone za pomocą rozwiązań mobilnych – by mogły być powszechnie stosowane i rozwijane – muszą być niezawodne i bezpieczne. Dlatego coraz większą wagę przywiązuje się nie tylko do poprawy parametrów transmisji i wzrostu funkcjonalności urządzeń, ale także do zapewnienia wysokiego poziomu ochrony systemów teleinformatycznych. Urządzenia mobilne bardzo często są wykorzystywane do przechowywania danych poufnych oraz do ich przesyłania, co potwierdzają także wyniki przeprowadzonej ankiety dotyczącej użytkowania urządzeń mobilnych, których omówienie jest zamieszczone w artykule. Autorzy podkreślili wagę problemu bezpieczeństwa użytkowania urządzeń mobilnych wobec dynamicznego rozwoju nowych technologii i wzrostu zagrożeń sieciowych.

Słowa kluczowe: łączność bezprzewodowa, urządzenia mobilne, zagrożenia dla systemów mobilnych

Wireless Internet Access in the Information Society – the Development and Threats

Summary

The numerous benefits of access to mobile Internet sparked great interest in wireless solutions, fostering their dynamic growth seen in recent years. The opportunities and increasing usage of mobile devices necessitate the development of new wireless standards to improve the quality of services. All technologies are systematically developed due to the need to ensure Interoperability between them, the need to increase the transmission speed and the need for efficient use of bandwidth. Activities undertaken with mobile solutions – in order to be widely used and developed – must be reliable and secure. That is why more and more attention is paid not only to improvements in transmission parameters and increased functionality of devices, but also to ensuring a high level of system protection. Mobile devices are often used to store and transmit confidential data, which is also confirmed by the results of the survey into the use of mobile devices, which is the topic of this article. The authors stress the importance of the problem of safety in mobile devices usage in the light of rapid development of new technologies and the increase in network threats.

Keywords: mobile devices, threats to mobile systems, wireless communication

JEL: M150, L860, C490