**Nierówności Społeczne a Wzrost Gospodarczy, nr 52 (4/2017)**
DOI: 10.15584/nsawg.2017.4.34 **ISSN 1898-5084**

*dr inż. Teresa Mendyk-Krajewska*[1]
Katedra Informatyki, Wydział Informatyki i Zarządzania
Politechnika Wrocławska

# Bezpieczeństwo urządzeń mobilnych w aspekcie realizacji e-usług

## Wprowadzenie

Wygodne w użytkowaniu, rozbudowane funkcjonalnie urządzenia mobilne, udostępniające usługi multimedialne i komunikacyjne w różnych technologiach, są dziś powszechnie stosowane i generują coraz więcej ruchu internetowego.

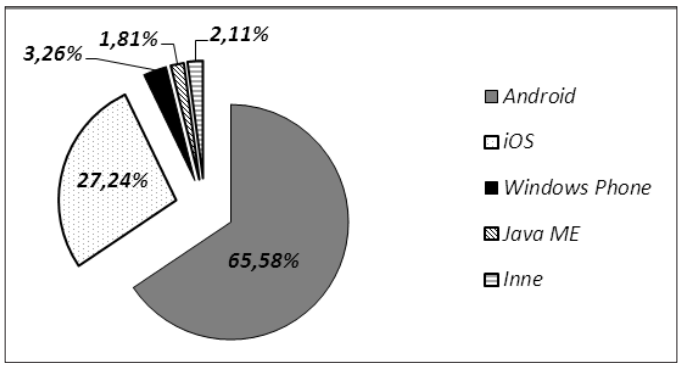
Wraz z rozwojem e-usług (z zakresu administracji publicznej, działalności gospodarczej, sądownictwa itd. – ich lista jest stale poszerzana) i przynoszącego korzyści ekonomiczne e-biznesu, urządzenia mobilne przechowują i przesyłają coraz więcej ważnych danych. Są to hasła dostępowe, dane osobowe i kontaktowe, wiadomości, zdjęcia, pliki dźwiękowe i wideo oraz dane biznesowe. Rozwój technologii bezprzewodowych i prognozowany wzrost ruchu internetowego pochodzącego z urządzeń mobilnych kieruje na nie uwagę cyberprzestępców. Zagrożenie dla wykorzystywania urządzeń mobilnych do realizacji usług drogą elektroniczną może stwarzać niewłaściwe ich użytkowanie, wadliwa aplikacja lub szkodliwe oprogramowanie.

Najpopularniejszym urządzeniem mobilnym jest obecnie smartfon, a najczęściej wykorzystywaną platformą systemową Android. W kolejnych jej wersjach wprowadzone zostały liczne modyfikacje, także związane z bezpieczeństwem, jednak nieustanny wzrost zagrożeń wymusza dalsze działania w tym kierunku. Celem artykułu jest ukazanie mechanizmów ochrony platformy Android oraz wskazanie zasad bezpiecznego użytkowania urządzeń mobilnych coraz powszechniej wykorzystywanych do realizacji e-usług (w tym płatności elektronicznych) i zadań biznesowych. Szkodliwe kody są tworzone głównie dla tego systemu, dlatego rozważania dotyczące bezpieczeństwa zostały ograniczone do tej platformy.

[1] Adres korespondencyjny: Politechnika Wrocławska, Wydział Informatyki i Zarządzania, Katedra Informatyki, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław; tel.713203969; e-mail: teresa.mendyk-krajewska@pwr.edu.pl.

## Platforma systemowa Android i jej aplikacje

Rynek urządzeń mobilnych został zdominowany przez platformę systemową Android firmy Google przeznaczoną na smartfony, telefony komórkowe, tablety i netbooki. Rynkowy udział mobilnych systemów operacyjnych przedstawiono na rys. 1 (dane z czerwca 2016 r.) [Mobile/Tablet Operating System Market (http)]. Na popularność systemu Android wpłynęły takie czynniki jak: niezależność sprzętowa[2], otwartość kodu, możliwość personalizacji urządzenia, integracja z usługami firmy Google[3] oraz dostępność dużej liczby aplikacji, przy relatywnie niskich kosztach.




**Rys. 1. Rynkowy udział mobilnych systemów operacyjnych**

Źródło: opracowanie własne na podstawie: www.netmarketshare.com.

Na drugim miejscu popularności znalazł się system iOS firmy Apple (27,24%), kolejno, ale daleko za nim, są systemy Windows Phone (3,26%) i Java ME (1,81%). Udział pozostałych systemów (Symbian, BlackBerry, Samsung i innych) wynosi łącznie 2,11%.

W celu dokonania oceny wiedzy użytkowników na temat realnych zagrożeń dla wykorzystywania urządzeń mobilnych, m.in. do realizacji e-usług, w czerwcu 2016 roku zostało przeprowadzone autorskie badanie ankietowe w grupie 85 studentów informatyki Politechniki Wrocławskiej. Uzyskane wyniki, które przedstawiono pod koniec opracowania, potwierdzają też powszechność użytkowania platformy Android. Wśród ankietowanych posiadanie urządzenia z tym systemem zadeklarowało 81% użytkowników. Inne wykorzystywane systemy to: Windows Phone i iOS – po 6% oraz Windows Mobile, Symbian i BlackBerry mające po 2% użytkowników.

[2] System jest instalowany na urządzeniach mobilnych takich producentów jak: Samsung, Huawei, Sony, HTC oraz LG.

[3] Założenie konta Google pozwala użytkownikom na synchronizację z takimi usługami jak: Gmail, wyszukiwarka Google, Google Play czy Google+.

Według firmy Google najczęściej używanymi wersjami Androida są: KitKat (37,8%), Jelly Bean (29%) oraz Lollipop (25,6%)[4] [Czechowicz, (http)]. Z badań wynika, iż nowe wydania platform systemowych zyskują zainteresowanie stosunkowo wolno – najnowsze oprogramowanie Android 6.0 Marshmallow było w posiadaniu zaledwie 0,3% użytkowników.

System Android pojawił się dopiero w 2008 roku i od tego czasu jest systematycznie rozwijany. Stopniowo rozbudowywano funkcjonalność urządzeń o kolejne funkcje, takie jak odtwarzanie muzyki, nagrywanie filmów, nawigację (z wykorzystaniem map Google'a) czy realizację płatności zbliżeniowych (dzięki technologii NFC – *Near Field Communication*). Zmodyfikowano programistyczny interfejs aplikacji API (*Application Programming Interface*) pozwalający wykorzystywać możliwości systemu i urządzenia oraz wprowadzono mechanizmy zwiększające szybkość działania aplikacji. Urządzenia mobilne często wyposażone są w kompas, sensory motoryczne (czujniki przyspieszenia, pola magnetycznego, temperatury, odległości od określonego miejsca, czy siły nacisku) oraz akceleratory grafiki 3D.

Architektura platformy Android oparta jest na systemie operacyjnym Linux i składa się z czterech głównych warstw:
– Kernel Layer, którą tworzy jądro Linuxa dostosowane do smartfonów,
– Runtime Layer, na którą składają się biblioteki natywne i wirtualna maszyna Dalvik,
– Framework – która umożliwia korzystanie m.in. z funkcji nawiązywania połączeń oraz dostęp do plików i systemu GPS,
– warstwy aplikacji – tworzonej przez uruchomione procesy i aktywności komunikujące się z niższymi warstwami za pomocą API.

System Android obsługuje różne technologie komunikacyjne (Bluetooth, GSM, LTE, NFC, Wi-Fi) i formaty plików oraz udostępnia narzędzie OpenGL ES[5]. Do przechowywania danych wykorzystywana jest relacyjna baza danych SQLite.

W systemie Android aplikacje budowane są z komponentów (każdy posiada własny identyfikator URI – *Union Resource Identifier*), takich jak:
– Activity[6] – z reguły reprezentuje pojedynczy widok w aplikacji i ma umożliwić użytkownikowi interakcję z nią; każda aktywność może uruchomić inną,
– Service – do wykonywania zdalnych lub długo trwających operacji,
– Intent – definiuje intencje wykonania czynności (jedyny nie stanowi punktu wejścia w aplikacji),
– Broadcast Receiver – odpowiada na wysłane wiadomości typu Intent,
– Content Provider – dostarcza interfejs programistyczny API do wykonywanych operacji na gromadzonych danych.

[4] Dane z października 2015 r., publikowane na oficjalnej stronie developer.android.com.

[5] API dla grafiki 3D, dostępne też w systemach Symbian i iOS.

[6] Podczas działania może znajdować się w jednym z trzech stanów: Resumed (stan wykorzystywania aktywności), Paused, Stopped.

Aplikacje z reguły uruchamiane są jako osobne procesy Linuxa. Czasem życia procesów zarządza system, na podstawie wiedzy o dostępnej pamięci, uruchomionych programach oraz ich priorytetach. Ponieważ aplikacje są zbudowane z różnych powiązanych ze sobą komponentów, mogą mieć kilka punktów wejścia, co wpływa na ich bezpieczeństwo.

Podstawowym miejscem publikacji oraz dystrybucji aplikacji dla systemu Android jest internetowy sklep Google Play. Stanowi on największą platformę udostępniającą oprogramowanie na urządzenia mobilne, którą cechuje ujednolicenie tworzenia aplikacji, łatwość aktualizacji dostępnych programów użytkowych, duża ich różnorodność oraz utrudnienie tworzenia nielegalnych kopii. Błędom aplikacji na platformę Android sprzyja łatwość tworzenia oprogramowania i jego dystrybucji, jednak jest ono mniej restrykcyjnie weryfikowane pod względem bezpieczeństwa niż aplikacje przeznaczone dla platformy iOS[7] urządzeń iPhone oraz iPad firmy Apple.

## Model bezpieczeństwa platformy Android

Model bezpieczeństwa Linuxa wykorzystuje koncepcję tworzenia jednoznacznie identyfikowanych użytkowników należących do określonych grup, przy czym każdy może należeć do wielu z nich. Właścicielowi pliku oraz grupie, do której należy plik, a także pozostałym użytkownikom, przydzielane są odpowiednie uprawnienia: do odczytu, modyfikacji i zapisu pliku oraz uruchamiania.

Każda aplikacja w systemie Android jest zapisana i uruchamiana jako odrębny użytkownik należący do grupy o określonych uprawnieniach. Unikatowy identyfikator jest jej nadawany w momencie instalacji (w postaci pakietu) na urządzeniu. System uprawnień określający funkcje przyznane każdej z zainstalowanych aplikacji jest jednym z ważnych elementów modelu bezpieczeństwa, jednak wiele programów może pobierać dane użytkownika i je wykorzystywać w sposób nieupoważniony. W Androidzie aplikacje są uruchamiane w odizolowanym środowisku, jednak system może przydzielać im dodatkowe uprawnienia (np. w celu udostępnienia Internetu lub karty pamięci).

Uprawnienia stanowią osobną grupę użytkowników opisaną unikatowym identyfikatorem i muszą być zdefiniowane przez programistę w odpowiednim pliku (Android Manifest.xml). Wszystkie niezbędne dla systemu informacje o zainstalowanych na urządzeniu pakietach zawarte są w wyznaczonym katalogu (/data/system). Każdemu z pakietów przypisane są elementy (<perms>) zawierające nazwy (mapowane do identyfikatorów grup) przyznawanych uprawnień [Drak, Fora i in., 2015, s. 52–55]. Tym samym aplikacje uzyskują dostęp do zasobów umożliwiających korzystanie jedynie z wybranych funkcji systemu (próba użycia innych powoduje blokadę danej aplikacji).

[7] Bazuje na systemie operacyjnym Mac OS X 10.5 i tym samym jądrze.

Lista wymaganych przez aplikację uprawnień zostaje wyświetlona na ekranie urządzenia w chwili podjęcia próby jej instalacji. Brak zgody użytkownika na udostępnienie określonych funkcji oznacza rezygnację z użytkowania danego oprogramowania[8].

Ponieważ procesy i zasoby różnych programów w systemie Android są od siebie odizolowane – dla potrzeb komunikacji pomiędzy aplikacjami, a także między komponentami jednej aplikacji, udostępniany jest mechanizm IPC (*Inter-Process Communication*), stosowany m.in. z wykorzystaniem komponentów Intent[9] lub Binder[10] (wymaga implementacji interfejsu za pomocą języka AIDL – *Android Interface Definition Language*). Każdy komponent aplikacji powinien być odpowiednio zabezpieczony, a odbierane przez nią dane weryfikowane.

Zarówno użytkownicy aplikacji, jak i ich twórcy powinni mieć świadomość wagi przydzielania uprawnień. Częstym błędem programistów jest wymaganie przydzielenia aplikacji praw, które nie będą przez nią wykorzystywane. Z kolei użytkownicy zwykli akceptować uprawnienia mechanicznie, bez znajomości konsekwencji decyzji.

Jedną z wad systemu uprawnień jest zbyt mała granularność przyznawanych praw. Przykładem może być uprawnienie READ_CONTACTS, które dla systemu Android w wersji 4.0 (i wcześniejszych) pozwala na dostęp do listy kontaktów użytkownika oraz historii połączeń. Problem może powstać również w przypadku, gdy dwie aplikacje (jednego autora) o różnych uprawnieniach mogą się ze sobą komunikować, bowiem stwarza to możliwość nieupoważnionego przekazywania danych.

W systemie Android każda aplikacja musi zostać podpisana (z wykorzystaniem klucza prywatnego asymetrycznego algorytmu szyfrowania, np. RSA), by można było zweryfikować jej oryginalność z użyciem klucza publicznego, który jest dołączany do publikowanej aplikacji. Do tego celu można wykorzystać narzędzie jarsinger z pakietu JDK Javy (*Java Development Kit*)[11] [Darwin, 2013, s. 583–584]. Niestety, sprawdzenie certyfikatu następuje tylko jeden raz – w chwili instalacji aplikacji, co jest słabością rozwiązania.

W kolejnych wersjach platformy Android wprowadzane są coraz lepsze zabezpieczenia. W wersji 4.0 zastosowano losowy przydział przestrzeni adresowej ASLR (*Address Space Layout Randomization*) dla każdego procesu, w wersji 4.2 dodano wyświetlanie ostrzeżenia w przypadku wysyłania wiadomości gene-

[8] Użytkownicy Androida od wersji 6.0 mogą selektywnie przyznawać uprawnienia, ale nie mając gwarancji poprawnego działania aplikacji w przypadku braku wszystkich akceptacji.

[9] Umożliwia programowi wysłanie wiadomości do wszystkich uruchomionych aplikacji (lub wybranej); do ich odbioru służy komponent Broadcast Receiver (programista może wykluczyć odbieranie wiadomości od innych aplikacji).

[10] Dzięki sterownikom leżącym w warstwie jądra systemu komponent ten może nawiązać bezpieczną komunikację pomiędzy dowolnymi identyfikowanymi procesami.

[11] Pakiet zawiera również narzędzie Keytool do generowania pary kluczy; prywatny przechowywany jest na urządzeniu właściciela w odpowiednim pliku (Keystore) chronionym hasłem.

rującej wyższe koszty, umożliwiono korzystanie z połączeń VPN (*Virtual Private Network*), weryfikowanie aplikacji przed ich instalacją, a opisy uprawnień dostarczają więcej szczegółów o działaniu programów. Następnie wprowadzono kontrolę urządzenia mobilnego łączącego się z komputerem, poprzez potrzebę akceptacji przez użytkownika smartfonu wygenerowanego klucza, bez czego nie jest możliwa komunikacja za pomocą ADB (*Android Debug Bridge*). Kolejnym wdrożonym dla poprawy bezpieczeństwa rozwiązaniem był moduł SELinux (*Security Enhanced Linux*) będący zestawem zabezpieczeń w jądrze Linuxa ograniczających możliwość przydzielania aplikacjom dostępu do zasobów (od wersji Android 4.4 jest to obligatoryjne). W wersji 5.0 wprowadzono automatyczne szyfrowanie przechowywanych w urządzeniu danych oraz możliwość użytkowania urządzenia przez kilka osób (zakładania kont lub korzystania z urządzenia przez „gościa" – bez dostępu do danych i aplikacji).

W szóstej edycji systemu Android udoskonalono system przyznawania uprawnień aplikacjom, udostępniono API do weryfikowania użytkownika poprzez analizę linii papilarnych, wprowadzono wyświetlanie stosownych komunikatów w przypadku problemów z weryfikacją działającego systemu oraz dodano warstwę abstrakcji sprzętowej HAL (*Hardware Abstraction Layer*) stanowiącą ogniwo łączące sprzęt z jądrem systemu operacyjnego.

Android umożliwia przechowywanie danych na wiele sposobów, jednak dla wysokiego poziomu ochrony należy stosować ich szyfrowanie. W tym celu można wykorzystać biblioteki SQL Cipher lub Secure-Preferences, gdzie dostępny jest symetryczny szyfr blokowy AES, a jedną z opcji jest szyfrowanie całego dysku.

## Zagrożenia dla urządzeń mobilnych

Urządzenia mobilne nie mogą być postrzegane jako w pełni bezpieczne, mimo wprowadzania coraz bardziej złożonych mechanizmów ochrony. Tym samym powstaje pytanie o bezpieczeństwo realizowanych z ich wykorzystaniem usług. Zagadnienie to nabiera istotnego znaczenia w dobie intensywnej informatyzacji Polski obserwowanej w ostatnich latach. W sektorze publicznym (administracji, służbie zdrowia, sądownictwie itd.) wdrażane są różnego rodzaju platformy informatyczne (systematycznie poszerzany jest też zakres udostępnianych e-usług), zaś obywateli zachęca się do ich powszechnego użytkowania. Tymczasem obawy o bezpieczeństwo usług realizowanych drogą elektroniczną są w pełni uzasadnione. Wiele zagadnień – w tym identyfikacja obywateli (stosowany Profil Zaufany nie we wszystkich zastosowaniach można uznać za bezpieczny) i ochrona ich danych osobowych – dotąd nie zostało właściwie rozwiązanych. Użytkownicy narażeni są na liczne zagrożenia, takie jak przekiero-

wanie na fałszywą stronę internetową (co może skutkować przejęciem poufnych danych) i utrudnienia (np. blokadę dostępności usług w wyniku ataku DoS).

Problemem bezpieczeństwa sieciowego zajmuje się wiele organizacji, m.in. OWASP (*Open Web Application Security Project*). Na opublikowanej przez nią liście aktualnych zagrożeń dla aplikacji mobilnych znalazły się między innymi: słabe mechanizmy zabezpieczeń procesów autoryzacji i uwierzytelniania, niewystarczająca ochrona warstwy transportowej, niezabezpieczenie komponentów IPC, możliwość wstrzykiwania danych po stronie klienta oraz modyfikacji aplikacji, po uzyskaniu dostępu do jej kodu źródłowego.

W systemie Android wiele informacji potrzebnych do podjęcia ataku można uzyskać dzięki inżynierii wstecznej lub analizie logów. Częstym źródłem infekcji urządzeń jest aplikacja zawierająca dodatkowo szkodliwy kod. Sposoby uzyskania nieuprawnionego dostępu do danych lub wykorzystania urządzenia do bezprawnych działań rozwijane są wraz ze wzrostem funkcjonalności urządzeń. Przykładem może być wykorzystanie technologii NFC (dostępnej w Androidzie od wersji 2.3) do podejmowania ataków poprzez podmianę kodów i przekierowanie połączenia na stronę zainfekowaną.

Szkodliwe oprogramowanie może umożliwiać śledzenie działań użytkownika (jego połączeń, lokalizacji, przekazywanych wiadomości, wykonywanych zdjęć itp.), pobieranie danych, modyfikację parametrów konfiguracyjnych lub wysyłanie wysoko płatnych wiadomości. Zagrożenie dla smartfonów stanowi pobieranie danych osobowych i kontaktowych oraz informacji o samym urządzeniu (takich jak: jego model, numery IMEI[12], IMSI[13], czy wersja systemu).

Liczba zagrożeń dla urządzeń mobilnych z systemem Android stale rośnie. Z raportu firmy Alcatel-Lucent wynika, że w 2014 roku odnotowano 25-procentowy wzrost zainfekowanych urządzeń mobilnych (było ich 16 mln, z czego 99% działało pod kontrolą Androida) w stosunku do roku poprzedniego [Wasilewska-Śpioch, (http)].

Jednym z przykładów nowego szkodliwego oprogramowania jest Shedun (występujący w kilku wersjach, działający z prawami administratora i ukrywający się pomiędzy plikami systemowymi), dystrybuowany za pomocą zmodyfikowanych aplikacji. Shedun uzyskuje dostęp do danych użytkowanych aplikacji oraz procesów systemowych i jest bardzo trudny do usunięcia [*Użytkownicy Androida zagrożeni...,* (http)]. Groźnym zagrożeniem jest też koń trojański Android. Toorch.1.origin (wbudowany w aplikację latarki), który po zainstalowaniu próbuje uzyskać uprawnienia roota, by móc ładować, instalować i usuwać aplikacje urządzenia. Przesyła też pod wskazany adres informacje o zainfekowanym urządzeniu, takie jak: bieżąca lokalizacja, numer identyfikacyjny, wersja platformy systemowej czy dostępność aktywnego połączenia WiFi [*Kolejny wirus na*

[12] International Mobile Equipment Identity – unikatowy numer identyfikacyjny używany przez sieć GSM.

[13] International Mobile Subscriber Identity – numer identyfikujący kartę SIM.

*smartfonach...*, (http)]. Oprogramowanie to instaluje szkodliwe moduły do katalogu systemowego, który nie jest skanowany podczas szybkiej kontroli programem antywirusowym, co utrudnia jego wykrycie.

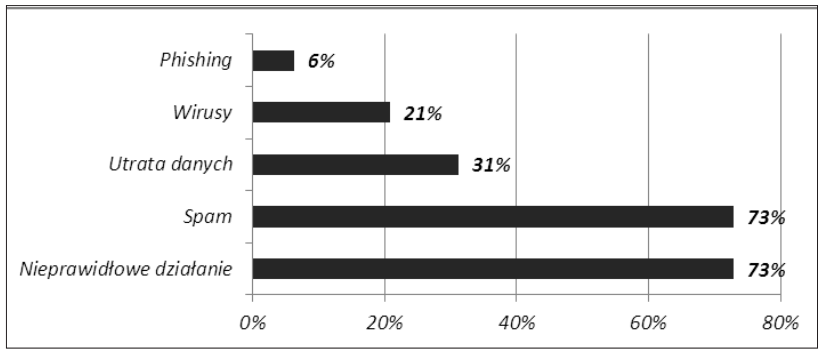
Jeszcze innym przykładem nowego szkodliwego oprogramowania dla urządzeń mobilnych jest koń trojański GM Bot (inne nazwy to: Bankosy, MazarBot) opisany przez CERT jesienią 2015 roku, który m.in. rozsyła wiadomości sms, usuwa dane i przekazuje realizowane połączenia. Drogą infekcji urządzenia może być kliknięcie linku w otrzymanej wiadomości lub instalacja aplikacji zawierającej szkodliwy kod [*mBank ostrzega...,* (http)]. Przed GM Bot'em ostrzegał swoich klientów mBank, gdyż program przesyła pobrane dane na serwery kontrolowane przez przestępców. Ten szkodliwy kod skutecznie podszywający się pod instytucje finansowe wykrywa aż 68 aplikacji bankowych różnych firm, w tym także polskich banków [*Banki ostrzegają klientów…,* (http)].

Głównym celem ataków są systemy firmowe (w szczególności instytucji finansowych), serwisy aukcyjne, sklepy internetowe oraz agendy rządowe. Wyjątkowo interesujące dla przestępcy może być przejęcie kontroli nad urządzeniem mobilnym osoby zajmującej ważne stanowisko.

W kwietniu 2016 roku Rada Bankowości Elektronicznej Związku Banków Polskich wydała oficjalny komunikat, w którym przestrzega użytkowników przed nasilającymi się atakami na smartfony z systemem Android, których celem jest wyłudzenie danych dostępu do kont bankowych. Z raportu CERT Orange Polska za rok 2015 wynika, że próby nieautoryzowanego dostępu do kontrolowanych przez instytucje systemów stanowią ok. 20% wszystkich niepożądanych zdarzeń w sieci [Nowy Raport CERT, (http)]. W celu przeprowadzenia ataku przestępcy wykorzystują słabości mechanizmów ochrony urządzeń, z których użytkownicy łączą się z siecią firmy oraz prywatne profile pracowników na portalach społecznościowych. Koszty ataków internetowych są wciąż relatywnie niskie (potencjalne zyski mogą je przekraczać wielokrotnie), zaś ryzyko poniesienia konsekwencji prawnych nadal niewielkie.

Urządzenia mobilne z powodu małych rozmiarów są podatne na zgubienie lub kradzież. Doświadczyło tego 15% objętych wspomnianą autorską ankietą studentów. Do najczęściej deklarowanych problemów należą: otrzymywanie spamu i nieprawidłowe działanie urządzenia (dotyczy 73% ankietowanych). Procentowy rozkład zagrożeń odnotowanych przez objętych badaniem użytkowników przedstawiono na rys. 2. Mimo ryzyka – oprogramowanie ochronne o pełnej funkcjonalności, umożliwiające m.in. zdalne kasowanie plików, identyfikację położenia urządzenia oraz identyfikację i usuwanie plików – wykorzystuje jedynie 17% ankietowanych.

Choć użytkownicy rejestrują niepożądane incydenty i mają wysoką świadomość istnienia realnych zagrożeń (deklaruje ją 90% ankietowanych), aż 52% badanych przesyła poufne dane, a 27% przechowuje je w pamięci urządzenia.




**Rys. 2. Rejestrowane przez ankietowanych zagrożenia**

Źródło: opracowanie własne.

Jedną z głównych przyczyn problemów ochrony urządzeń przed zagrożeniami są błędy oprogramowania. W styczniu 2016 r. odkryto poważną lukę w systemie Linux pozwalającą zwiększyć przywileje użytkownika do poziomu roota przy pomocy specjalnie spreparowanego kodu (tzw. exploita)[14]. Takie błędy oprogramowania usuwa się poprzez aktualizację systemu, czyli instalację wydanej przez producenta nakładki (w możliwie szybkim czasie), jednak w przypadku platformy Android jest to również zależne od producentów urządzeń [Kotowski, (http)].

Dla zmniejszenia ryzyka warto posługiwać się urządzeniem wyposażonym w najnowszą wersję platformy systemowej i przestrzegać podstawowych zasad bezpieczeństwa, czyli:
– odpowiednio skonfigurować urządzenie,
– nie przechowywać w pamięci urządzenia ważnych informacji,
– przesyłać dane bezpiecznym kanałem,
– wyłączyć niewykorzystywane technologie i usunąć nieużywane aplikacje,
– nie instalować aplikacji z niepewnego źródła,
– sprawdzać, do jakich informacji żąda dostępu pobierana aplikacja,
– nie pobierać plików z niezaufanych stron WWW i nie podawać na nich swoich danych,
– kontrolować poprawność adresów odwiedzanych stron internetowych,
– korzystać z najmocniejszych dostępnych metod uwierzytelniania,
– poprawnie kończyć nawiązywane sesje,
– tworzyć kopie zapasowe ważnych plików,
– weryfikować prawdziwość informacji pochodzących od banków,
– używać oprogramowanie antywirusowe (umożliwiające też zdalne śledzenie sprzętu oraz blokowanie lub usuwanie znajdujących się na nim danych).

[14] Błąd dotyczy systemów wykorzystujących kernel od wersji 3.8.

Znani producenci oprogramowania, m.in. Juniper Junos Pulse, Trend Micro Mobile Security i Websense Triton Mobile Security opracowali dla urządzeń mobilnych specjalistyczne zabezpieczenia, kierując ofertę w stronę e-biznesu [*Urządzenia mobilne bezpieczne...,* (http)].

## Podsumowanie

W dobie rozwoju społeczeństwa informacyjnego, realizowanie różnego rodzaju usług drogą elektroniczną z wykorzystaniem urządzeń mobilnych staje się koniecznością. Jedną z przyczyn dotąd niewielkiego zainteresowania użytkowników zdalnym dostępem do opracowanych platform systemowych, obok problemów z ich poprawnym działaniem (przerwy techniczne, nieustannie wprowadzane zmiany), jest obawa o bezpieczeństwo realizacji e-usług.

Wobec rosnących zagrożeń i z powodu roli, jaką dziś odgrywają w życiu codziennym i biznesie – urządzenia mobile są coraz lepiej chronione. O ich bezpieczeństwo powinni dbać również sami użytkownicy przestrzegając określonych reguł użytkowania, stosując dostępne zabezpieczenia techniczne i programowe. Różne organizacje nadzorujące problematykę bezpieczeństwa sieciowego oraz producenci narzędzi ochrony cyklicznie publikują raporty o aktualnym stanie zagrożeń oraz przewidywanych trendach ich rozwoju. Obserwowana tendencja wzrostowa niepożądanego zjawiska wymusza wypracowywanie coraz to doskonalszych zabezpieczeń.

Kwestię bezpieczeństwa należy traktować priorytetowo, bowiem od niego w znacznym stopniu zależy zakres i stopień wykorzystywania dynamicznie budowanych w ostatnich latach systemów teleinformatycznych w instytucjach publicznych, a także dalszy rozwój e-usług.

## Bibliografia

Czechowicz B., 2015, *Lillipop jest zainstalowany na co czwartym urządzeniu z systemem Google*, http:// pclab.pl/news66801.html (dostęp: 15.05.2016 r.).

Darwin I.F., 2013, *Android. Receptury*, Wyd. Helion, Gliwice.

Drake J.J., Fora P.O., Lanier Z., Mulliner C., Ridley S.A., Wicherski G., 2015, *Android. Podręcznik hackera*, Wyd. Helion, Gliwice.

http://superbiz.se.pl/nowoczesne-technologie/banki-strzegaja-klinetow-uwaga-na-sms-y-ze-zlosliwym-oprogramowaniem_820243.html (dostęp: 20.05.2016 r.).

http://technowinki.onet.pl/oprogramowanie/mbank-ostrzega-uzytkownikow-telefonow-z-systemem-android/rs00t7 (dostęp: 17.04.2016 r.).

http://www.clico.pl/edukacja/artykuly/urzadzenia-mobilne-bezpieczne-dla-biznesu (dostęp: 5.07.2016 r.).

Kotowski A., 2016, *Znaleziono poważną lukę w Linuxie*, http://pclab.pl/news67999.html (dostęp: 20.02.2016 r.).

NetMarketShare, Mobile/Tablet Operating System Market Share. www.netmarketshare.com (dostęp: 20.06.2016 r.).
Nowy Raport Cert Orange Polska, 2016, https://cert.orange.pl/aktualnosci/nowy-raport-cert-oran (dostęp: 15.06.2016 r.).
softonet.pl/publikacje/aktualnosci/Uzytkownicy.Androida.zagrozeni.zlosliwym.prawie.niemozliwym.do.usuniecia.oprogramowaniem,1425 (dostęp: 17.12.2015 r.).
tech.wp.pl/kat,130054,title,Kolejny-wirus-na-smartfonach,wid,17477841,wiadomości.html (dostęp: 17.07.2016 r.).
Wasilewska-Śpioch A., 2015, *Zagrożenia mobilne – co musisz o nich wiedzieć, żeby skutecznie się obronić*, http://di.com.pl/zagrozenia-mobilne-co-musisz-o-nich-wiedziec-zeby-skutecznie-sie-obronic-52293 (dostęp: 20.05.2016 r.).

*Streszczenie*

Powszechnie używane urządzenia mobilne przechowujące różnego rodzaju dane są obecnie wykorzystywane nie tylko do prowadzenia rozmów telefonicznych i przesyłania krótkich komunikatów, ale też do korzystania z zasobów internetowych, realizacji e-usług oraz zadań biznesowych. Zagrożenie dla ich bezpieczeństwa może stwarzać niewłaściwe ich użytkowanie, wadliwe oprogramowanie lub szkodliwe kody. Utrzymanie wysokiego poziomu ochrony tych urządzeń stanowi poważny problem. Najpopularniejszym urządzenie mobilnym jest smartfon, a najczęściej wykorzystywanym oprogramowaniem system Android. W artykule opisano tę platformę systemową i wbudowane mechanizmy ochrony, wskazano realne zagrożenia dla urządzeń mobilnych oraz przedstawiono zasady bezpiecznego ich użytkowania.

*Słowa kluczowe:* platforma Android, ochrona smartfonów, zagrożenia urządzeń mobilnych

**Security of mobile devices in aspect of e-services**

*Summary*

Commonly used mobile devices that store all kinds of data are now being used not only to make phone calls and send short messages, but also to make use of online resources and e-services, as well as for business tasks. The threat to their security can be caused by their improper use, faulty software or malicious code. Maintaining a high level of protection for these devices is a serious problem. The most popular mobile device is a smartphone, and the most widely used software system is Android. The article describes this system platform and its built-in protection mechanisms, indicates a real threat to mobile devices and presents principles of safe usage.

*Keywords:* Android platform, smartphones security, mobile device threats

JEL: O300, O320, O390