

*Katarzyna Lange-Sadzińska**

STANDARDY BEZPIECZEŃSTWA W SIECIACH BEZPRZEWODOWYCH WI-FI

Wprowadzenie

Rozwój EDI i EC wymusza poszukiwanie coraz nowszych, tańszych i bardziej elastycznych rozwiązań komunikacji. Technologie komunikacyjne dla EDI i EC muszą zapewniać przede wszystkim bezpieczeństwo. Dlatego właśnie każda nowa technologia jest sprawdzana i tak szeroko dyskutowana pod tym względem.

W niniejszym artykule przedstawię jeden ze sposobów korzystania z Internetu (np. w USA jest wykorzystywany w ok. 3% gospodarstw domowych). Tym sposobem jest transmisja bezprzewodowa z wykorzystaniem fal radiowych. Zasada nie jest nowa, natomiast wyzwaniem było zapewnienie odpowiedniej szybkości przesyłania danych i bezpieczeństwa przy kosztach porównywalnych z tradycyjnymi sieciami. Spełnienie tych wymagań pozwoliło wykorzystać atuty sieci wynikające z bezprzewodowości.

Sieci bezprzewodowe trzeba stosować wszędzie tam, gdzie konieczne jest zachowanie mobilności sprzętu (np. komputery przenośne w magazynach czy innych „ruchomych” stanowiskach pracy). Sieci bezprzewodowe pozwalają na podłączenie komputerów przenośnych do lokalnej sieci LAN firmy. Ponadto można wykorzystać taką sieć wszędzie tam, gdzie nie można poprowadzić kabli pod ziemią. W wielu sytuacjach poprowadzenie kabli jest niemożliwe, np. ze względu na zabytkowy charakter budynku. Sieć bezprzewodowa idealnie sprawdza się przy aranżacji kilkudniowych instalacji na czas trwania wystawy czy targów.

Przy opisie sieci radiowych używa się dwu określeń: Wi-Fi (Wireless Fidelity) i WLAN (Wireless LAN).

W 1997 r. organizacja IEEE (Institute of Electrical and Electronic Engineers) ustanowiła normę 802.11 definiującą „radiowy ethernet” znany pod nazwą Wireless LAN (WLAN). WLAN jest to zespół urządzeń komunikujących się ze sobą drogą radiową za pomocą specjalnych adapterów nadawczo-odbiorczych.

Dzięki Wi-Fi Alliance [16] – organizacji skupiającej producentów

* Dr, adiunkt, Zakład Informatyki Ekonomicznej, Uniwersytet Łódzki.

oprogramowania i sprzętu do sieci radiowych – został wylansowany na rynkach całego świata system sieci bezprzewodowej o nazwie Wi-Fi, skrót od Wireless Fidelity (bezprzewodowa wierność). Wi-Fi jest nieodłącznie związana z standardem 802.11. Dokładnie standard 802.11b nazywany jest powszechnie Wi-Fi.

Standard IEEE 802.11 określa zasady pracy urządzeń do transmisji bezprzewodowej w sieciach lokalnych. Normuje zatem modemy bezprzewodowe, platformy API, urządzenia PCMCIA, mosty między przewodowymi i bezprzewodowymi sieciami LAN. W dokumentach standaryzacyjnych zawarte są zasady bezpieczeństwa danych przesyłanych bezprzewodowo, eliminowanie zakłóceń nadawania, protokoły komunikacji z urządzeniami docelowymi za pomocą fal radiowych lub podczerwonych.

Standard IEEE 802.11 został zaakceptowany przez ETSI¹ pod nazwą ETS 300328. Poniżej przedstawione zostały główne zalety i wady sieci Wi-Fi (opracowanie własne na podstawie [1]).

Zalety sieci Wi-Fi:

- Technika Wi-Fi pozwala założyć sieć komputerową bez konieczności kucia ścian i przeciągania kabli. Jednocześnie można ją połączyć z siecią kablową LAN.
- Każdy właściciel przenośnego komputera albo innego urządzenia wyposażonego w interfejs Wi-Fi może skorzystać w każdej chwili z Internetu (w Polsce – na razie tylko w wybranych miejscach).
- Sieć Wi-Fi jest prosta w montażu i daje duże możliwości rozbudowy

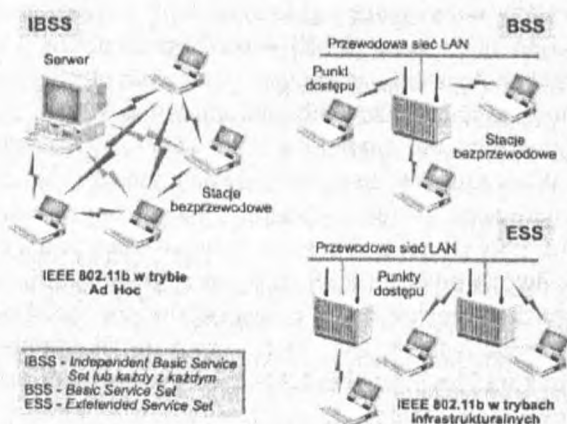
Wady sieci Wi-Fi:

- Na razie jeszcze uważana jest za drogą technologię
- Ciągłe jeszcze rozwiązania różnych producentów nie są ze sobą kompatybilne.
- Przy projektowaniu sieci trzeba wybierać miejsca, w których na drodze sygnału nie będzie większych przeszkód

¹ ETSI (European Telecommunication Standard Institute, czyli Europejski Instytut Normacyjny do spraw Telekomunikacji) utworzony w 1988 r., z siedzibą w Sophia-Antipolis we Francji.

Topologie sieci Wi-Fi

Właściwie w przypadku sieci bezprzewodowych jest trochę niezręcznie używać słowa topologia. Przyzwyczajenie każe nam szukać topologii fizycznych połączeń (których tutaj nie widać...). Pozostając jednak przy tym tradycyjnym określeniu możemy wskazać na trzy [12] podstawowe topologie sieci Wi-Fi. Zostało to zobrazowane na rys. 1.



Rys. 1. Trzy topologie sieci Wi-Fi

Źródło: strony <http://www.wirelesslan.pl/>,
<http://www.networkworld.pl/suplementy/wlan/wlan.html>

Pierwszą z topologii jest IBSS (Independent Basic Service Set) – sieć niezależna (tymczasowa, *ad hoc*) odpowiada klasycznej sieci *peer-to-peer*, w której nie wyróżnia się żadnego urządzenia pełniącego funkcję serwera. Sieć *ad hoc* nie posiada elementów stałych. Sieci tymczasowe tworzone są zazwyczaj na czas spotkania, konferencji itp. Składają się one z pewnej liczby komputerów przenośnych, które mogą wymieniać między sobą informacje.

IBSS (Independent Basic Service Set) wymaga komputera z radiową kartą sieciową. Każda stacja nadawczo-odbiorcza posiada ten sam priorytet i komunikuje się z innymi komputerami bezpośrednio, bez żadnych dodatkowych urządzeń aktywnych. Maksymalna odległość między stacjami w tym przypadku wynosi od 30 do 60 m. We wszystkich urządzeniach musi być ustawiony ten sam identyfikator domeny (Wireless Domain ID), umożliwiający

komunikację tylko z wybranymi maszynami i zabezpieczający przed nieautoryzowanym dostępem do naszej sieci.

BSS (Basic Service Set) – konfiguracja, w której oprócz stacji bezprzewodowych występuje przynajmniej jeden komputer (punkt dostępowy²) służący do komunikowania się ze zwykłą, przewodową siecią. Taka konfiguracja jest najczęściej wykorzystywana w sieciach korporacyjnych. Zazwyczaj mamy w nich do czynienia z wieloma bezprzewodowymi stacjami roboczymi, które połączone są w grupy komunikujące się z różnymi punktami dostępowymi albo sprzętem wpiętym do sieci stałej. Kiedy zachodzi konieczność wymiany danych między urządzeniami, informacje przesyłane są np. na drodze komputer z kartą Wi-Fi – punkt dostępowy – sieć kablowa – drukarka. Punkty dostępu są połączone przewodem sieciowym i pełnią w przybliżeniu funkcje stacji bazowych telefonii komórkowej.

Ostatnia topologia sieci opartej na 802.11 to ESS (Extended Service Set) – sieć złożona. W istocie jest to zestaw dwóch lub więcej „komórek” BSS, tworzących pojedynczą sieć dzięki połączeniom kablowym lub bezprzewodowym. ESS (Extended Service Set) powstaje podczas połączenia ze sobą co najmniej dwóch podsieci BSS. Wystarczy połączyć ze sobą HUB-y AP (pełniące podobną funkcję jak huby w sieciach przewodowych) tradycyjnym okablowaniem umożliwiając w ten sposób komunikację stacjom bezprzewodowym z tradycyjną siecią LAN oraz z jednostkami znajdującymi się w innych podsieciach radiowych.

Rozwój standardu

Na opis standardów obowiązujących w sieciach bezprzewodowych czy choćby tylko radiowych należałoby poświęcić osobną pracę [11]. Oprócz tych najbardziej znanych i często wymienianych, czyli 802.11, 802.11a, 802.11b, istnieje cała gama opatrzona literkami od „e” do „o”. Na potrzeby niniejszego opracowania przedstawię podstawowe standardy komunikacji radiowej ze szczególnym uwzględnieniem tych, które dotyczą bezpieczeństwa. Inne zagadnienia potraktuję z konieczności skrótowo.

Obecnie występują następujące standardy sieci WLAN [13]:

1. Pierwszy z nich, zgodny z normą IEEE 802.11, pozwala na osiągnięcie maksymalnej przepustowości 2 Mb/s (przy większych odległościach prędkość spada do 1 Mb/s). Maksymalna odległość pomiędzy urządzeniami nadawczymi ściśle zależy od jakości podzespołów wyprodukowanych przez producenta. Ogólnie przyjmuje się, że wartość ta powinna zawierać się w granicach 30-60 m w

² Punkt dostępu (*access point*, *hot-spot*, *hub* AP) pośredniczy w transmisji między siecią przewodową i bezprzewodową.

pomieszczeniach zamkniętych i do kilkuset metrów na otwartej przestrzeni przy komunikacji niezależnej. Dzisiaj norma ta jest rzadko stosowana.

2. Popularna obecnie modyfikacja IEEE 802.11b zezwala na transmisję z prędkością 11 Mb/s w promieniu 25 m w pomieszczeniach zamkniętych. Przy większych odległościach ze względu na liczbę błędów transfer spada do 5 Mb/s. Na otwartych przestrzeniach odległość nie powinna być większa niż 250 m (rozwiązanie to jest dostępne w Polsce dopiero od końca 2000 r. i charakteryzuje się dość wysoką ceną w stosunku do wersji kablowej). Najnowsza modyfikacja normy 802.11b zezwala na transmisję do 22 Mbit/s, jednak potrzebne są do niej całkowicie nowe urządzenia.

3. Istnieje też technologia Wi-Fi5, która odpowiada standardowi 802.11a i różni się od poprzedniej zakresem częstotliwości – 5 GHz oraz prędkością transmisji, która może wynosić do 54 Mb/s. Zaletami tego standardu jest mniejsze obciążenie sieci radiowej i większa prędkość. Jego ograniczone zastosowanie może wynikać z wysokiej ceny, o połowę mniejszego zasięgu, który wynosi do 50 m, większego poboru prądu oraz braku kompatybilności ze standardem 802.11b.

4. Nowością obecnie jest specyfikacja 802.11g³ zezwalająca na pracę do 54 Mbit/s nadal w częstotliwości 2,4 GHz. 802.11g – standard sieci bezprzewodowej o wysokiej prędkości – jest kompatybilny z wolniejszym 802.11b. Niestety, praca z nominalną przepustowością wymaga silnych anten lub ogranicza zasięg stosowania samego sprzętu.

Bezpieczeństwo

Grupy robocze [14] IEEE 802.11 pracujące nad poszczególnymi standardami dla sieci bezprzewodowych, koncentrowały się na zagadnieniach takich, jak prędkość, bezpieczeństwo i optymalizacja wykorzystania częstotliwości.

Grupa Robocza G została powołana dla zwiększenia przepustowości (22 Mbps lub więcej) w paśmie 2.4 GHz bez potrzeby rezygnowania z istniejącej infrastruktury sieci 802.11b.

Grupa Robocza A została powołana do zapewnienia przepustowości 54 Mbps w paśmie 5 GHz.

³ Standard 802.11g został ratyfikowany 11.06.03 w Instytucie Inżynierii Elektryki i Elektroniki (IEEE).

Grupa Robocza H zajmowała się rozwiązywaniem problemów interferencji i kolizji sygnałów w medium radiowym. Specyfikacja 802.11h⁴ wymaga od urządzeń, aby sprawdziły przed transmisją, czy dana częstotliwość jest w użyciu.

Grupa Robocza E została powołana, aby zmienić zasady kolejkowania pakietów. W 802.11b każdy pakiet ma taką samą szansę na transmisję. Grupa Robocza E miała za zadanie to zmienić, aby zagwarantować niektórym pakietom wyższy priorytet niż innym. Jest to zadanie niesłychanie trudne, ale potrzebne dla transmisji głosu (z użyciem Voice Over IP VoIP⁵). 802.11e mógłby być zastosowany jako uzupełnienie różnych standardów IEEE, w tym b, g, i a. Pakiety głosowe miałyby nadawany priorytet w określonych odstępach czasu, co gwarantuje ciągłość rozmów.

System szyfrowania WEP

Zadaniem Grupy Roboczej I było poprawienie bezpieczeństwa.

System szyfrowania WEP (Wireless Equivalent Privacy) wbudowany w 802.11b posiadał wiele słabych punktów. Należało znaleźć zamiennik dla WEP, jednocześnie zapewniając poprawną pracę użytkowników korzystających z dotychczasowego systemu WEP.

Pierwszy etap prac polegał na „poprawieniu” technologii WEP, aby zapobiec możliwości przechwycenia kilku megabajtów danych i odczytania (wyekstrahowania) kluczy WEP (to ulepszenie dałoby gwarancję, że złamanie szyfru zajmowałoby ok. 100 000 lat przy dzisiejszych możliwościach obliczeniowych).

Niestety, nie udało się wyeliminować innych słabości systemu WEP.

W związku z tym drugi etap prac polegał na zastąpieniu szyfrowania WEP nowym systemem. Nazwano go TKIP (Temporal Key Integrity Protocol). Nazwa ta opisuje zastosowaną technologię: klucze zachowują swą tajność przez dany czas. Dodatkowo zakłada się rotację kluczy w krótkich odstępach czasu. Tak powstał standard 802.11i.

⁴ 802.11h została sformułowana na potrzeby użycia pasma 5 GHz na terenie Europy. Wynikało to z konieczności zagwarantowania możliwości stosowania tego pasma na rynku europejskim, przy lansowaniu przez Unię Europejską standardu HiperLAN2, odmiennego od 802.11a. W tej sytuacji 802.11a połączone z 802.11h może być stosowane na rynku europejskim.

⁵ Voice over Internet Protocol – pakietowy przekaz głosowy (możliwe są rozmowy telefoniczne przy wykorzystaniu podłączenia do Internetu).

System szyfrowania WPA

Użytkownicy są zainteresowani przede wszystkim tym, czy standard 802.11i będzie konsekwentnie stosowany w urządzeniach różnych producentów. Dlatego z zadowoleniem popierają wszelkie inicjatywy na rzecz ujednolicania standardu bezpieczeństwa. Największe zasługi ma tu Wi-Fi Alliance, która promuje ujednolicony standard bezpieczeństwa jako Wi-Fi Protected Access (WPA).

WPA określa się jako wstęp do docelowej wersji 802.11i. Nową specyfikację wspierają m.in. firmy D-Link, NetGear i Linksys.

Użytkowanie sieci Wi-Fi jest wygodne nie tylko dla użytkowników, ale również dla włamywaczy. Oferowane zabezpieczenia nie dadzą obronić się w 100%. Dlatego przyszli użytkownicy sieci bezprzewodowej muszą rozważyć dodatkowe fizyczne zabezpieczenie środowiska pracy sieci. Wśród ostatecznych środków zaradczych może znaleźć się nawet zastosowanie elektromagnetycznego ekranowania biura.

Dodatkowo należy pamiętać, że oprócz niebezpieczeństwa nieautoryzowanego dostępu do usług czy przechwycenia wiadomości wysyłanych drogą radiową istnieje jeszcze jedno zagrożenie. Jest to niebezpieczeństwo zablokowania dostępu do sieci uprawnionym użytkownikom. Można to zrobić uzyskując nieautoryzowane połączenie z punktem dostępowym poprzez sieć stacjonarną, a następnie zmianę ustawień tego punktu. Ochrona w takich przypadkach zależy od mechanizmów bezpieczeństwa w aplikacjach AP (punktów dostępowych).

Przykłady wdrożeń Wi-Fi na świecie

Wi-Fi w pokojach hoteli Marriott [17]. Firma Marriott International udostępniła w swoich hotelach łączność z Internetem Wi-Fi już w 2002 r. Usługa będzie dostępna w 400 hotelach sieci Marriott. Dalsze plany firmy dotyczą wprowadzenia Wi-Fi do publicznie dostępnych miejsc, jak np. sale konferencyjne.

Wi-Fi na lotniskach [16]. T-Mobile, amerykańska filia Deutsche Telekom w porozumieniu z Borders Group i Starbucks udostępniła usługę w 2 tys. punktów na terenie Stanów Zjednoczonych. Pomysł skierowany do linii American Airlines, Delta Air Lines and United Airlines zapewni dostęp do sieci Wi-Fi w ok. 100 klubach i poczekalniach na terenie USA. Miejsca te zapewnią biznesmenom i osobom podróżującym łatwy dostęp do poczty elektronicznej.

Wi-Fi w pociągu [18]. Od połowy października 2003 r. na dwóch trasach francuskich pociągów TGV pasażerowie mogą korzystać w bezprzewodowego dostępu do Internetu w standardzie Wi-Fi dzięki inicjatywie przewoźnika

i firmy IBM. Z łączności Wi-Fi można korzystać na trasach Paryż – Bordeaux oraz Bordeaux – Pau, obsługiwanych przez podróżujące z prędkością 300 km/h pociągi TGV. Na czas podróży można wypożyczyć laptopa od przewoźnika. Na razie hot-spoty (punkty dostępowe) w pociągach są uruchomione na roczny okres próbny.

Wi-Fi na dworcu [3]. W Wielkiej Brytanii rozszerza się rynek usługodawców Wi-Fi. British Telecom i Megabeam powiększają liczbę miejsc, w których będzie można skorzystać z tej technologii łączności z siecią. Wi-Fi ma się pojawić na stacjach kolejowych: Euston Station, Liverpool Street Station, Waterloo Station i Victoria Station w Londynie, na lotniskach London City i John Lennon w Liverpoolu oraz w sieci hoteli Moat House w Edynburgu, Glasgow, Gatwick, Manchesterze, Cambridge Garden, Harlow/Stansted, Oakley Court i Shepperton. Łącznie z działającymi już trzema punktami – na Paddington Station, Reading Moathouse i Hammersmith – Megabeam będzie łącznie posiadał 17 miejsc z dostępem do Wi-Fi.

Podobne działania podejmuje firma BT Openzone, która posiada już 36 miejsc z dostępem do Wi-Fi. Miejsca te są zlokalizowane głównie w hotelach, centrach biznesowych czy siedzibach korporacji.

Wi-Fi na boisku [10]. Firma Toshiba zamierza uruchomić począwszy od 2003 r. bezprzewodowe punkty dostępu do Internetu w 72 klubach piłkarskich w Wielkiej Brytanii. Pierwszy, testowy hot-spot pojawił się w Reading. Brytyjscy fani piłki nożnej i dziennikarze sportowi będą mogli skorzystać z Internetu podczas oglądania meczu (przesyłanie szybkich relacji, zdjęć z przebiegu rozgrywek).

Wi-Fi w barze. Przy współpracy firmy Toshiba powstały także hot-spoty w barach McDonald's w Stanach Zjednoczonych.

Technologia Wi-Fi w Polsce

Uregulowania prawne. Na mocy rozporządzenia Ministerstwa Infrastruktury z dnia 6 sierpnia 2002 (DzU, 02.138.1162) częstotliwość 2,4 GHz została zwolniona z wszelkich opłat, można więc korzystać z sieci Wi-Fi bez żadnych ograniczeń. Uporządkowanie Krajowej Tablicy Przeznaczeń Częstotliwości miało również na celu zastosowanie Wi-Fi jako alternatywnego kanału dostępu do abonentów telekomunikacyjnych w miastach, co popiera Urząd Regulacji Telekomunikacji i Poczty.

18 listopada 2003 rozpoczął się w Krakowie Tydzień z Technologią Bezprzewodową [7]. Atrakcją był zorganizowany przez firmę Intel, wraz z producentami komputerów przenośnych Toshiba, IBM, Dell, Fujitsu Siemens, Hewlett-Packard oraz z dostawcą produktów bezprzewodowych Xylab, najgłębszy w Europie punkt dostępowy. W kopalni soli w Wieliczce na

głębokości ponad 300 m pod ziemią w Komorze Warszawa zaproszeni goście mogli się bezprzewodowo połączyć z Internetem.

Drugi, bardziej praktyczny przykład pochodzi z Wrocławia [6]. W wyniku współpracy Urzędu Miasta Wrocławia i krakowskiej firmy Xylab w listopadzie 2003 r. uruchomiona została usługa bezpłatnego bezprzewodowego dostępu do Internetu na terenie wrocławskiej Starówki, dzięki radiowej technologii Wi-Fi. Teraz nawet pod gołym niebem – dosłownie i w przenośni – na ławce lub w kawiarnianym ogródku będzie można odwiedzić swoje ulubione strony WWW bądź sprawdzić pocztę. Planuje się uruchomienie Wi-Fi na placu Grunwaldzkim we Wrocławiu, wokół którego mieszka większość studentów.

Literatura

- [1] Bednarczyk M., Krygier J., *Bezpieczeństwo sieci bezprzewodowych 802.11b*, <http://www.enter.pl/info/archiwum.asp>
- [2] Borisov N., Goldberg I., Wagner D., *(In)Security of the WEP algorithm* <http://www.isaac.cs.berkeley.edu/isaac/wep-slides.pdf>
- [3] *Ekspansja Wi-Fi*, artykuł z e-laptop.pl pod adresem: <http://www.e-laptop.pl/modules.php?name=News&file=article&sid=195>
- [4] Kroplewski P., *WPA czyli WI-FI PROTECTED ACCESS*, INTERLINE <http://www.interline.pl/interline.php?s0=&s1=1&s2=1&s00=1&s01=1&sx=2&s=czytelnia/wpa>
- [5] Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2003.
- [6] Kuźmiński P., *Bez kabla i za darmo*, 5.11.2003, źródło: Wrocławski Serwis Internetowy http://newsroom.chip.pl/news_73907.html
- [7] Kuźmiński P., *Najgłębszy hotspot w Europie*, <http://webpl.org/?page=index&ile=al>
- [8] Matthew S. Gast, *802.11. Sieci bezprzewodowe. Przewodnik encyklopedyczny*, Helion, Gliwice 2003.
- [9] Nowicki K., Woźniak J., *Przewodowe i bezprzewodowe sieci LAN*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2002.
- [10] Orszewski R., *Wi-Fi na boisku*, <http://www.fkn.pl/avantgo/>
- [11] Pliszka J., *Przewodnik po sieciach bezprzewodowych (802_11b Wi-Fi)*, 3.7.2003. <http://www.interneo.pl/FAQ/book1.html>
- [12] Rudziński A., *Zerwać druty*, 8.26.2003 <http://magazyn.chip.pl/>
- [13] *Sieci radiowe Wireless LAN*, artykuł ze strony <http://www.wirelesslan.pl/>
- [14] *Standard IEEE 802_11*, artykuł ze strony <http://sakul.terramail.pl/spis.html>
- [15] *System sieci bezprzewodowej - WI-FI*, AXED <http://www.axed.com.pl/wifi.htm#top>
- [16] *Wi-Fi na lotniskach*, artykuł z e-laptop.pl pod adresem: <http://www.e-laptop.pl/modules.php?name=News&file=article&sid=178>
- [17] *Wi-Fi w pokojach hotelowych*, artykuł ze strony <http://www.4d.pl/show.php?id=1827>
- [18] *WI-FI w pociągu*, artykuł ze strony <http://www.enter.pl/info/archiwum.asp?id=2339>
- [19] Zieliński B., *Bezprzewodowe sieci komputerowe*, Helion, Gliwice 2000.

Katarzyna Lange – Sadzińska

Security standards of wireless networks Wi-Fi

Summary

This paper describes Wi-Fi, a kind of wireless communication. Wi-Fi idea is especially good for mobile computers into the LAN. However this paper describes problems of data security in wireless networks. The main problem is possibility of interception the messages.