

REKOMENDACIJA DĖL PRIVATUMO APSAUGOS NAUDOJANTIS BELAIDŽIAIS TINKLAIS

BELAIDŽIAI TINKLAI IR JŲ TECHNOLOGIJOS, KAS TAI?

Belaidžiai tinklai (angl. *Wireless Local Area Network (WLAN)*) yra alternatyva tradiciniams laidiniams tinklams. Belaidžiai tinklai dėl pigumo ir palygint greito bei paprasto įdiegimo tapo prieinami ir privatiems asmenims. Jie padeda asmeniui tapti mobiliam (galimybė naudotis internetu biure, namuose), suteikia greitą ir patogią prieigą, komforto pojūtį, sumažina tinklo įdiegimo ir eksploatavimo sąnaudas.

Belaidžio greitą ir patogią kompiuterinio tinklo technologija (angl. *Wireless Fidelity (WiFi)*) suteikė galimybę sukurti infrastruktūrą mobilaus interneto ryšio tiekimui. Teritorija, kurioje yra įdiegta belaidžio tinklo infrastruktūra, vadinama ryšio zona (angl. *HotSpot*). Pastaruoju metu sparčiai plinta viešai prieinamas belaidis internetas, kurio plėtrą lemia interneto vartotojų mobilumas, galimybė juo naudotis dažniausiai lankomose viešose vietose (degalinėse, kavinėse, parduotuvėse, pagrindinėse gatvėse ir t. t.). Norėdamas prisijungti prie viešai prieinamo belaidžio interneto, asmuo turi:

- Turėti nešiojamą kompiuterį, kuriame būtų įdiegta belaidžio ryšio tinklo korta, atitinkanti belaidžio tinklo (WiFi IEEE-802.11b) ryšio standartą, ir reikiama programinė įranga.
- Būti belaidžio interneto zonoje (pažymėtoje *HotSpot* ženklu).

Ryšio zonos, kuriose įdiegtas belaidžio tinklo (WiFi IEEE-802.11b) ryšio standartas, užtikrina patikimą ir greitą ryšį. Belaidžio tinklo technologija gali būti naudojama kompiuteriams vienas su kitu sujungti, prijungti prie interneto ar įprastų laidinių kompiuterių tinklų.

Tarptautinė duomenų apsaugos telekomunikacijose darbo grupė (www.datenschutz-berlin.de) dokumentu „Dėl galimos rizikos privatumui, naudojantis belaidžiais tinklais“ (priimtu 35-ajame darbo grupės susitikime) kreipėsi į Elektros ir elektronikos inžinierių instituto (angl. *Institute of Electrical and Electronics Engineers (IEEE)*) Belaidžių tinklų darbo grupę, *WiFi* aljansą ir belaidžių įrenginių pardavėjus su prašymu atkreipti dėmesį į privatumo ir saugumo problemas plėtojant belaidžio ryšio tinklų technologijas.

Lietuvos standartas LST ISO/IEC:17799:2006 numato, kad prieigos prie belaidžių tinklų atveju turėtų būti taikomos papildomos tapatybės nustatymo valdymo priemonės. Belaidžių tinklų valdymo priemonės turi būti parenkamos ypač atidžiai, kadangi jais naudojantis atsiranda kur kas daugiau galimybių nepastebimai įsibrauti į tinklu siunčiamų duomenų srautą ir perimti informaciją.

Belaidžiai tinklai turėtų būti atskirti nuo vidinių ar privačių tinklų. Atsižvelgiant į tai, kad belaidžių tinklų ribas nėra lengva tiksliai apibrėžti, turėtų būti atliktas rizikos vertinimas, kuriuo turėtų būti nustatytos tinkamos tinklų atskyrimo valdymo priemonės (pavyzdžiui, patikimas tapatybės nustatymas, šifravimo būdai ar dažnio pasirinkimas).

BELAIDŽIŲ TINKLŲ PRIVATUMO IR SAUGUMO PROBLEMOS

Be minėtų privalumų, belaidžiai tinklai kelia ir grėsmių tinklo bei informacijos saugumui, asmens privatumui:

- Duomenys belaidžiuose tinkluose perduodami radijo bangų signalais, kurie sklinda erdvėje, todėl perimti duomenis yra daug lengviau negu įprastiniuose laidiniuose tinkluose (reikalinga kryptinė antena).
- Sudėtinga aptikti įsilaužėlių. Tai patogu įsilaužėliui, nes anonimiškumas beveik garantuotas ir yra maža rizika būti nubaustam.
- Žmonės nesuvokia įsilaužimo grėsmės. Daugelis įsigytos ir įjungtos į tinklą belaidės įrangos lieka veikti su neaktyvuotais saugumo nustatymais (nenaudojami prisijungimo slaptažodžiai, neįjungiamas šifravimas). Pavyzdžiui, palikti belaidžio tinklo prieigą su gamykliniais nustatymais – tai tas pats, kaip palikti atviras namo duris.

- Jeigu naudojama techniškai pasenusi įranga, daugeliu atvejų neužtikrinama tinkama tinklo apsauga. Saugumo priemonės pasenusios ir plačiai žinomos įsilauželiams. Pavyzdžiui, nerekomenduojama naudoti WEP (angl. *Wired Equivalent Privacy*) protokolo, kuris yra nesaugus, nes šifravimo algoritme buvo aptikta spragų.
- Belaidžių tinklų pažeidimo priemonės ir būdai yra viešai prieinami ir demonstruojami internete (pvz., *how to Crack WEP* (angl.)).

Kokios konkrečios grėsmės iškyla belaidžio tinklo naudotojams:

- Potencialus įsilaužėlis, skenuodamas belaidžiu tinklu siunčiamus duomenų paketus, gali atskleisti vartotojų vietos nustatymo ir asmens duomenis: vartotojo prisijungimo prie tinklo prieigos vardą ir slaptažodį, IP adresą ir kt.
- Privatumo pažeidimas: grėsmė siunčiamam pranešimo konfidencialumui ir vientisumui. Įsilaužėlis gali perimti siunčiamą pranešimą ar jį pakeisti.
- Duomenų vagystė arba sunaikinimas: įsilaužėlis belaidžio tinklo naudotojo asmeniniame kompiuteryje gali įdiegti kenkėjišką programą.
- Jei nesiimama tinkamų apsaugos priemonių, piktavaliai asmenys, esantys iki 100 m atstumu nuo belaidės įrangos (priklausomai nuo naudojamos įrangos charakteristikų), gali laisvai prisijungti prie belaidžio tinklo (įmonės ar privataus asmens) ir naudotis internetu nemokamai ar turėti prieigą prie bylų, o tinklo savininkas tam tikrą laiką gali to nė nepastebėti.
- Kenkėjiška programinė įranga: įsilaužėliai pasinaudoja svetimo tinklo resursais ir duomenimis neteisėtai informacijai platinti, įsilaužti į kitus tinklus ir pan.

REKOMENDACIJOS BELAIDŽIO TINKLO NAUDOTOJAMS

Belaidės tinklo įrangos pirkėją pardavėjas turėtų tinkamai informuoti apie belaidžių įrenginių saugumo nustatymus, kurie užtikrintų aukštą saugumo lygį ir konfidencialumą. Prieš nuspręsdami naudoti belaidžio tinklo technologijas, išigyti belaidę įrangą, pirkėjai turėtų įvertinti su privatumu susijusią riziką, kadangi jų pačių saugumo reikalavimai leis nuspręsti, kokia įranga yra tinkama.

Belaidės įrangos naudotojai, įsidiege minėtą įrangą (žr. priedo 1 paveikslą), turėtų imtis papildomų saugumo priemonių duomenų saugumui ir savo privatumui užtikrinti:

- Pakeisti nustatytą pradinį gamintojo slaptažodį, nes potencialūs įsilaužėliai, žinodami įrangos gamintojų naudojamus standartinius slaptažodžius, gali juos panaudoti neteisėtam prisijungimui (žr. priedo 2 paveikslą). Rekomenduojama, kad slaptažodyje, be raidžių ir skaičių, būtų ir bent keli specialūs simboliai. Slaptažodį rekomenduojama periodiškai keisti.
- Įjungti duomenų šifravimą. Šiuo metu moderniausios belaidžio tinklo apsaugos priemonės yra WPA (angl. *Wireless Protected Access*) ir WPA2 (angl. *Wireless Protected Access 2*) belaidžio tinklo saugumo protokolų rinkiniai, kuriuos palaiko naujesnės belaidžio ryšio įrangos programinės versijos (žr. priedo 3 paveikslą). Naudojant vieną iš šių saugumo protokolų, galima užtikrinti saugų radijo bangomis siunčiamų duomenų šifravimą.
- Išjungti belaidžio tinklo prieigos įrenginio signalą. Šis signalas į oro erdvę kas keletą sekundžių transliuoja tinklo identifikatorių (angl. *Service Set Identifier (SSID)*), kuris visada transliuojamas viešo ryšio zonose (*HotSpot*). Išjungę signalą, jūs tapsite nematomi, tad išibrovėliai negalės matyti jūsų asmeninio (ar įmonės) tinklo.


Naudojant minėtas saugumo priemones, tinklo pažeidžiamumo rizika bus žymiai mažesnė, bus labiau apsaugotas jūsų privatumas.

Dėl belaidžio interneto prieigos naudojimo, pvz., degalinėse, kavinėse, parduotuvėse ir kitose viešose vietose, reikėtų įsidėmėti, kad viešo ryšio zonose interneto teikimo būdas nėra saugus, kadangi nenaudojamos jokios saugumo priemonės. Duomenys, perduodami iš kompiuterio iki viešai prieinamo tinklo prieigos taško (angl. *access point*), nėra šifruojami. Asmenys, kurie

naudojasi belaidžio interneto prieiga viešose vietose, turėtų imtis papildomų saugumo priemonių savo saugumui ir privatumui užtikrinti:

- Šifruokite perduodamus elektroninio pašto pranešimus, junkitės tik prie saugių elektroninio pašto tinklalapių, kur veikia HTTPS, SSL ir kiti saugūs protokolai, pavyzdžiui, <https://webmail.xxx.lt>. Šiuo atveju vartotojo prisijungimo vardas ir slaptažodis bus perduotas saugiu kanalu į pašto serverį. Naudodamiesi saugos priemonėmis sumažinsite riziką nuo piktavališkų prisijungimų prie asmeninės pašto dėžutės.

- Nesiųskite atviru tekstu asmens duomenų (prisijungimo slaptažodžių, banko sąskaitų numerių ir t. t.), nes piktavaliai, pasinaudodami kenkėjiškomis programomis (angl. *man-in-the-middle*), gali perimti duomenų srautą, keliaujantį iš jūsų kompiuterio į paslaugų tarnybinę stotį. Todėl atliekant veiksmus su asmens duomenimis viešai prieinamame internete, rekomenduojama imtis ypatingų saugumo priemonių arba atsisakyti tokių operacijų.

- Pasinaudoję viešai prieinamu belaidžiu internetu, paspauskite kompiuterio belaidės posistemės mygtuką , taip jūsų kompiuteris taps nematomas belaidžio tinklo zonoje ir galėsite išvengti piktavališkų atakų, išnaudojančių belaidžių tinklų technologijų pažeidžiamumą.

- Naudokitės tik patikimais tinklais, nes belaidė posistemė automatiškai jungiasi prie bet kokio pasiekiamo belaidžio tinklo, jei nėra nustatyta kitaip. Į patikimų tinklų sąrašą, kuris saugomas nešiojamo kompiuterio atmintyje, reikėtų įtraukti tik saugių tinklų pavadinimus. Pasinaudojus atviru tinklu, reikėtų ištrinti atviro tinklo pavadinimą iš tinklų sąrašo (žr. priedo 4 paveikslą).

- Patikrinkite kompiuterio belaidės įrangos programos konfigūracijos nustatymus. Programos konfigūracijos lange (žr. priedo 5 paveikslą) išjunkite automatinį prisijungimą prie belaidžių tinklų (angl. *Automatically connect to non-preferred networks*) ir pasirinkite konfigūracijos nustatymą „Jungtis tik prie prieigos taškų“ (angl. *Access point (infrastructure) networks*). Taip įjungę kompiuterio belaidę posistemę, išvengsite automatiško prisijungimo prie bet kokio pasiekiamo belaidžio tinklo ir sumažinsite riziką užkrėsti savo kompiuterį kenkėjiška programa.

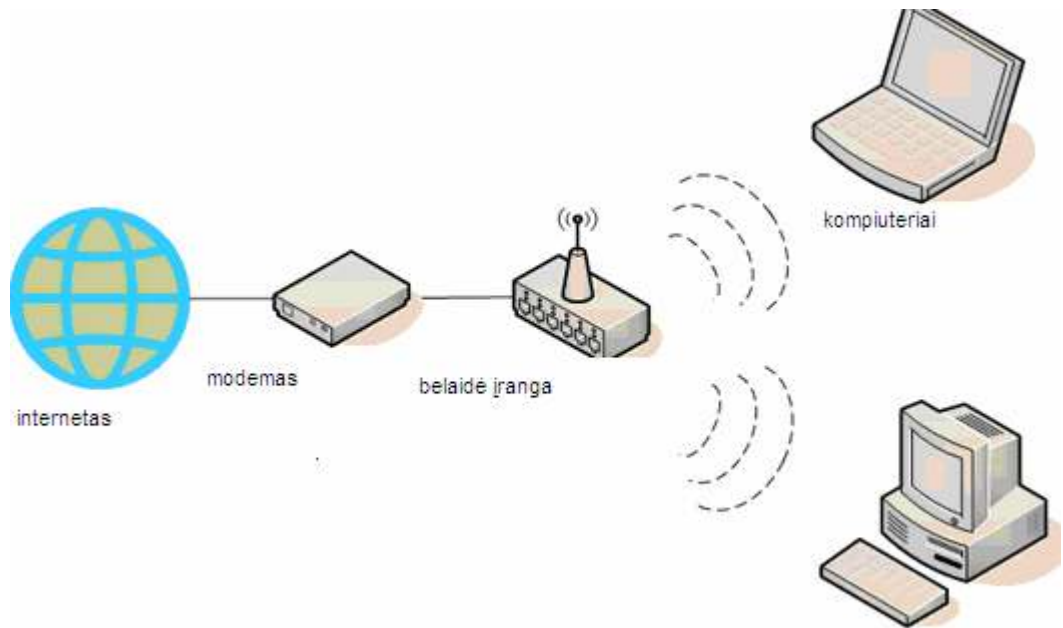
- Patikrinkite, ar jūsų kompiuteryje yra įjungta užkarda (angl. *firewall*). Pažymėkite varnele nustatymą, draudžiantį užkardos išimtis (angl. *dont allow exceptions*) (žr. priedo 6 paveikslą). Jei dalijimasis rinkmenomis bus uždraustas, tai jūsų duomenys bus neprieinami kitiems naudotojams, prisijungusiems prie to paties prieigos taško. Taip jūs labiau apsaugosite savo kompiuterį ir privatumą.

Parengė:

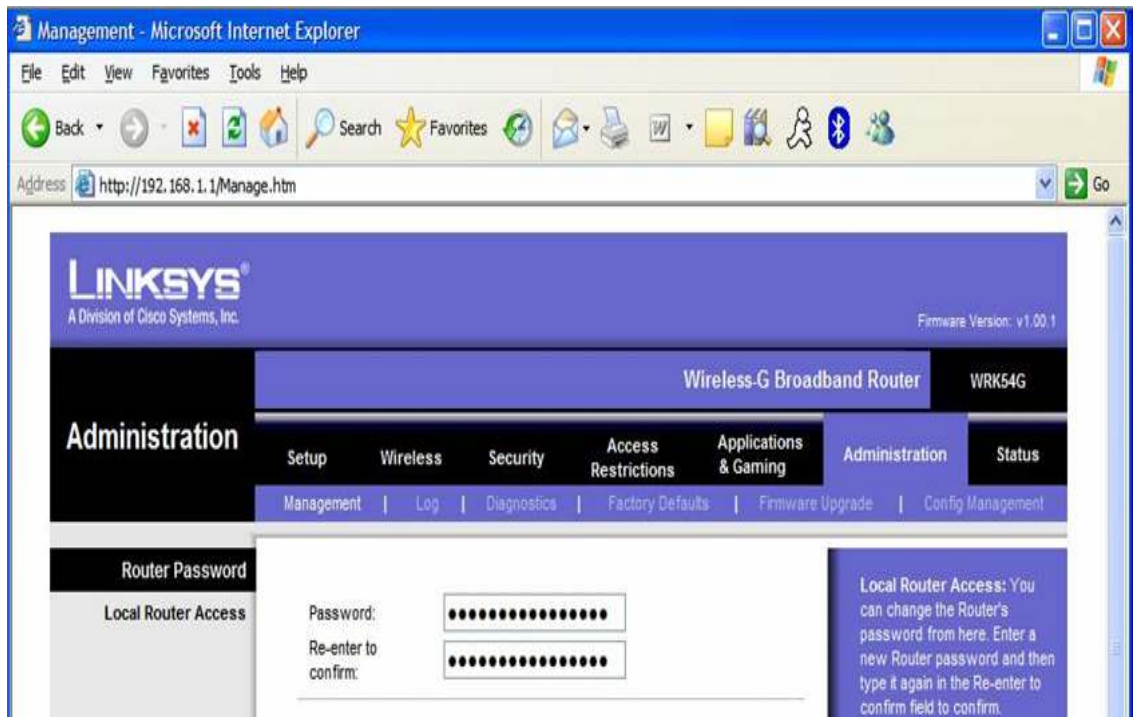
Valstybinės duomenų apsaugos inspekcijos

Informacijos ir technologijų skyriaus vyriausiasis specialistas

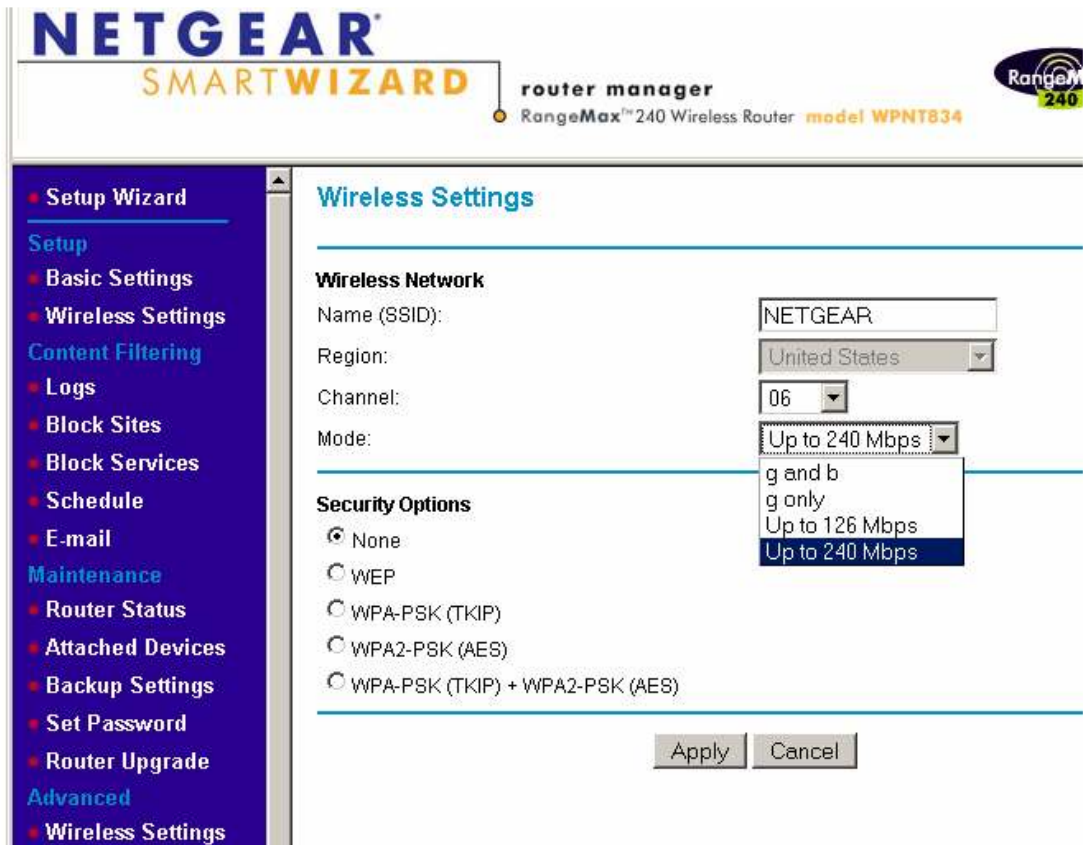
Zigmantas Medutis



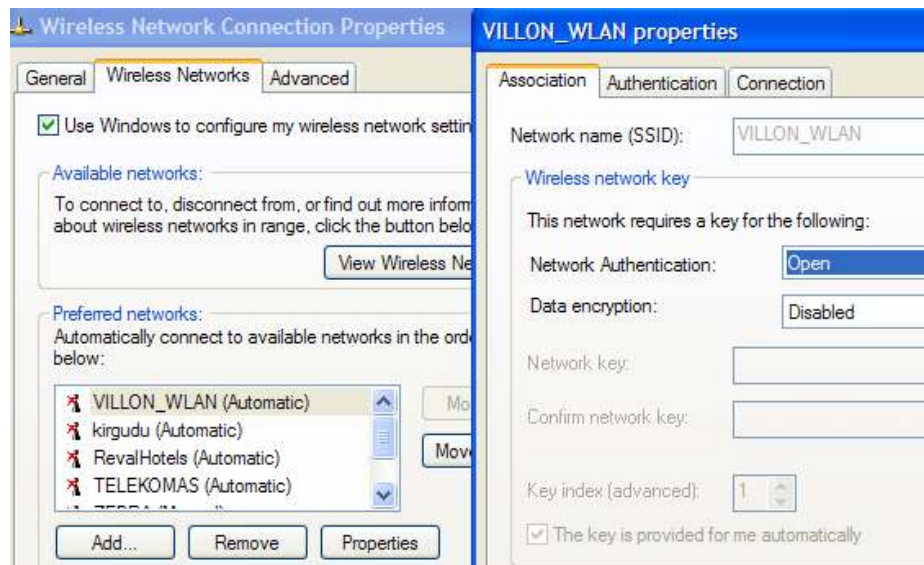
1 pav. Belaidės įrangos (maršruto parinktuvo) įjungimo schema



2 pav. Gamintojo slaptažodžio pakeitimas maršruto parinktuve



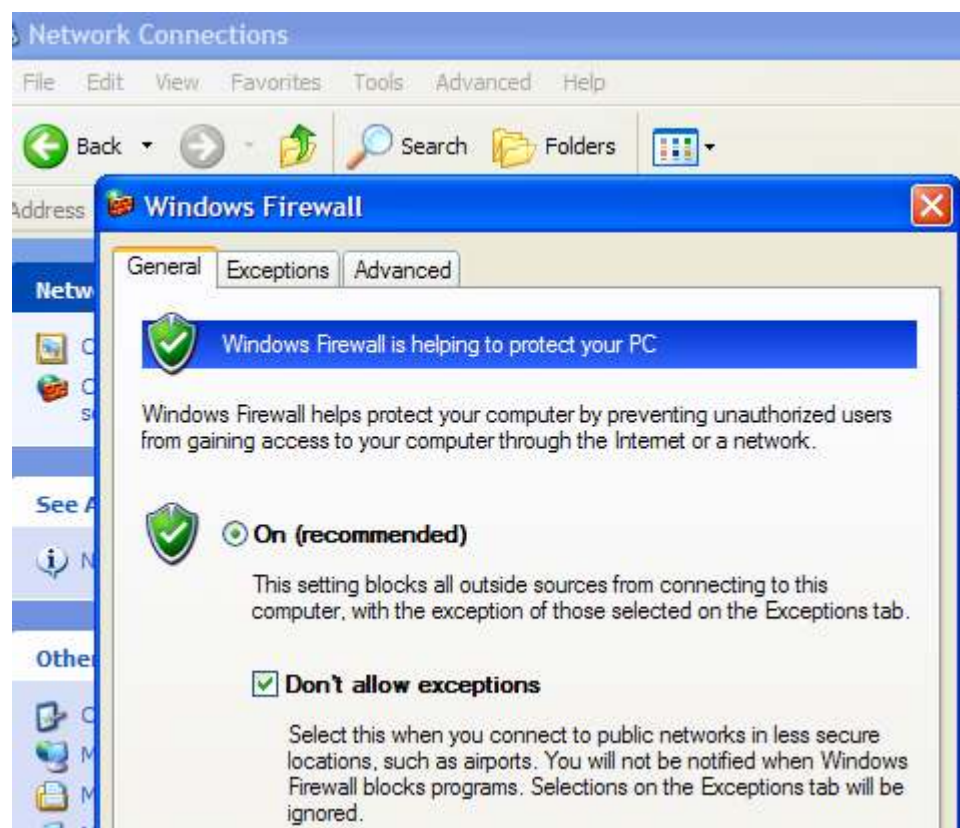
3 pav. Duomenų šifravimo nustatymas maršruto parinktuve



4 pav. Nesaugių (nešifruotų) tinklų šalinimas



5 pav. Belaidės įrangos programos konfigūracijos nustatymas kompiuteryje



6 pav. Užkardos įjungimas kompiuteryje

LITERATŪRA

1. International Working Group on Data Protection in Telecommunications. Working Paper on potential privacy risks associated with wireless networks. Main Recommendations (adopted at the 35th meeting, 2004). Prieiga internete <http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdp/working-papers-and-common-positions-adopted-by-the-working-group> (žiūrēta 2008-11-18).
2. IEEE 802.11 Working Group for Wireless Area Networks (WLANs). Prieiga internete <http://grouper.ieee.org/groups/802/11> (žiūrēta 2008-11-18).
3. NIST Publication 800-48: Wireless Network Security 802.11. Prieiga internete http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf (žiūrēta 2008-11-18).
4. Wi-Fi Wireless Fidelity. Prieiga internete <http://www.wi-fi.org/> (žiūrēta 2008-11-18).
5. Linksys WRT54GS Wireless-G Broadband Router with SpeedBooster. Prieiga internete <http://www.tomsguide.com/us/linksys-wrt54gs-wireless-wrt54gs.review-250-9.html> (žiūrēta 2008-11-18).
6. Wireless Security Initiative. Prieiga internete <http://spotlight.getnetwise.org/wireless/> (žiūrēta 2008-11-18).