Інформаційна безпека держави

УДК 621.391

Д.О. Волинець

Національна академія Державної прикордонної служби України ім. Б. Хмельницького, Хмельницький

ШЛЯХИ ЗБІЛЬШЕННЯ ЕНЕРГЕТИЧНОЇ ПРИХОВАНОСТІ РАДІОКАНАЛУ СТАНДАРТУ IEEE 802.11 ІТС ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

В умовах активного впровадження в оперативно-службову діяльність правоохоронних підрозділів мобільних засобів доступу до відомчих інформаційних ресурсів, значним зростанням використання мобільних радіотерміналів і мережевого радіообладнання, постає питання забезпечення безпеки використання бездротових каналів.

У дослідженні, на підставі моделі перехоплення радіосигналу, з метою досягнення максимального рівня енергетичної прихованості, формуються вимоги до радіосистеми стандарту IEEE 802.11 прикордонного підрозділу.

Ключові слова: *Гарт, АРМ, модель відкритих систем, енергетична прихованість, Wi-Fi канал, прихованість інформації, ймовірність виявлення сигналу,структура сигналу, сигнал/завада.*

Вступ

Постановка проблеми у загальному вигляді, її актуальність та зв'язок із важливими науковими чи практичними задачами. В умовах значного підвищення обсягу та важливості інформаційного забезпечення оперативно-службової діяльності підрозділів Державної прикордонної служби України, реалізацією якісно нового інформаційного насичення відомчої інтегрованої інформаційно-телекомунікаційної системи (ІІТС) «Гарт», впровадженням, в межах лібералізації візового режиму, доступу до ресурсів міжнародних правоохоронних структур (Європол, Interpol), постає питання організації надійних каналів передачі даних безпосередньо до автоматизованих робочих місць (АРМ) персоналу Держприкордонслужби України, які забезпечують перевірку та ідентифікацію осіб та транспортних засобів які перетинають Державний кордон України, а в умовах проведення антитерористичної операції на території окремих районів Донецької та Луганської області, в пунктах контролю в'їзду – виїзду (КПВВ) та на лінії розмежування з тимчасово окупованою АР Крим.

Крім значного зростання функціонального насичення складових ІІТС Держприкордонслужби «Гарт», на сьогоднішній день активно реалізується процес переходу на WEB-доступ низки спеціалізованих підсистем відомчої інтегрованої ІТС (ПС «Ризик», Гарт-НПД, ІТС «Гарт-5» та інші).

Окремо треба зазначити що питання організації надійних каналів передачі даних тісно пов'язано із процесом забезпечення підрозділів охорони кордону сучасними мобільними засобами автоматизації оперативно-службової діяльності, зокрема АРМ «Інспектор-К» із складу програмно-технічного комплексу (ПТК) автоматизації прикордонного контролю «Гарт-1/П» на базі мобільного комп'ютерного терміналу К.ВРТ500М, АРМ «Патруль» та «Дільничний інспектор» із складу ПТК автоматизації прикордонної служби «Гарт-3/П» на базі планшетного ПК СЕТ-10М.

Окрім питань щодо забезпечення необхідних швидкостей обміну даних та повноцінного використання функціональних можливостей відомчої інтегрованої інформаційно-телекомунікаційної системи на сьогоднішній день постають питання забезпечення захисту каналів передачі даних від існуючих загроз в системі інформаційного обміну.

Узагальнюючи різноманітні підходи, а також існуючі рішення в галузі кібербезпеки, вважаємо, що можна виділити такі основні види загроз:

– розкриття інформаційних ресурсів;

– порушення їх цілісності;

– збій в роботі обладнання.

Розглядаючи питання забезпечення безпеки каналу передачі даних в ланці «мобільне автоматизоване робоче місце – серверне обладнання» ми можемо стверджувати, що вирішуючи питання забезпечення оперативного доступу до інформаційних ресурсів Державної прикордонної служби з мобільних автоматизованих робочих місць, в першу чергу ми маємо вирішити питання безпеки організації та забезпечення цього доступу.

Незважаючи на велику кількість розроблених протоколів захисту інформації на верхніх рівнях

моделі відкритих систем OSI, ефективність їх значно знижується при передачі мультимедійної інформації [1–2]. Крім того, при активному впроваджені в оперативно-службову діяльність Державної прикордонної служби України цифрових технологій передачі інформації, забезпечити підвищення безпеки в каналах зв'язку тільки одними інформаційними (криптографічними) алгоритмами не представляється можливим.

Аналіз досліджень та публікацій. Окремо треба зазначити, що у вільному доступі нами не виявлено публікацій, які спрямовані на дослідження конфігурації і розмірів меж зон виявлення багатопроменевих каналів зв'язку. Відсутність цієї інформації перешкоджає розробці сучасних засобів і способів підвищення прихованості каналів зв'язку.

Метою даної статті є аналіз шляхів збільшення енергетичної прихованості Wi-Fi радіоканалу.

Виклад основного матеріалу

Прихованість релєєвських SISO каналів з квазистатичним загасанням досліджувалася в багатьох наукових роботах, в них, в якості критеріїв оцінки рівня прихованості, використовується ймовірність виявлення легітимного каналу $P_{в.}$ та гранична секретна продуктивність $C_{пр}=C_{л}–C_{відв}$, де $C_{л}$ та $C_{відв}$ – відповідно продуктивність легітимного и відвідного каналів. Канал рахується секретним, якщо $P_{виявл.}<0,7$ и $C_{пр}<0$.

В основу запропонованих досліджень покладена концепція відвідного каналу Вайнера [3], яка знаходить все більше застосування при дослідженні питань захисту інформації в цифрових системах зв'язку [4].

Враховуючи випадковий характер, як характеристик каналу зв'язку, так і можливостей порушника з протидії або перехоплення роботи легітимного каналу, критерій захищеності каналу зв'язку можна представити у формі ймовірність складної події $P_{з}$, яка є сумою двох елементарних подій: ймовірності прихованої роботи $P_{прих}$ та завадозахищеності каналу $P_{зз}$ [1]

$$\begin{gathered} P_{з} = P_{прих} + P_{зз} - P_{прих} \times P_{зз}; \\ P_{з} = 1 - P_{E} \times P_{\pi}, \end{gathered} \tag{1}$$

де $P_{E} = \left(1 - P_{прих}\right)$ – ймовірність виявлення каналу зв’язку; $P_{\pi} = \left(1 - P_{\pi з}\right)$ – ймовірність придушення каналу зв’язку завадою.

Оскільки ефективність заходів РЕП порушником в значній мірі залежить від виконання етапу виявлення каналу зв'язку, то розглянемо спочатку критерії оцінки прихованості системи зв'язку і визначимо шляхи її збільшення.

Як правило, радіотехнічна розвідка передбачає послідовне виконання трьох основних завдань: виявлення факту роботи радіосистеми (виявлення сигналу), визначення структури виявленого сигналу (на основі ряду його параметрів) і розкриття інформації яка міститься (передається) в сигналі [2].

Переліченим завданням виявлення каналу зв'язку порушником можуть бути протиставлені три види прихованості сигналів: енергетична, структурна та інформаційна [5]. У цьому випадку прихованість роботи каналу зв'язку можна оцінити ймовірністю прихованої роботи

$$P_{прих} = 1 - P_{E} \times P_{стр} \times P_{інф}, \tag{2}$$

де P_{E} – ймовірність виявлення сигналу чи факту функціонування каналу зв’язку;

$P_{стр}$ – ймовірність розкриття структури сигналу;

$P_{інф}$ – ймовірність розкриття змісту інформаційного сигналу.

Потрібно зауважити, що крім енергетичної прихованості існують ще ряд прихованостей, які спрямовані на виключення або істотне ускладнення виявлення сигналів системи зв'язку. Це – частотна, тимчасова, поляризаційна, просторова, маскувальна та інші види прихованості, які можуть виявлятися в різних поєднаннях і реалізуються на фізичному рівні каналу зв'язку.

Основними критеріями оцінки енергетичної прихованості каналу зв'язку крім ймовірності виявлення сигналу P_{E} при заданій ймовірності помилкової тривоги є відношення сигнал/завада на вході приймача зловмисника $\left(S/N\right)_{2}$, що забезпечує задану ймовірність виявлення P_{E} та радіус зони виявлення сигналу P_{E} при визначеному відношенні сигнал/завада на вході приймача зловмисника $\left(S/N\right)_{2}$.

Показник P_{E} застосовують для вирішенні низки практичних завдань, пов'язаних з розробкою організаційно-технічних заходів і визначенням розмірів контрольованих зон. Якщо припустити, що в приймачі-зловмиснику реалізовані оптимальні або квазіоптимальні алгоритми виявлення сигналів, то радіус зони виявлення можна наближено визначити виразом 3.

$$\begin{gathered} P_{E} = \frac{\lambda}{4\pi}\left[\left(P_{пер} \times G_{пер} \times G_{пр\,з}\right)\Big/ \right. \\ \left. \left(P_{пр\,з} \times FLS \times \left(S - N\right)_{2}\right)\right], \end{gathered} \tag{3}$$

де λ – довжина хвилі передавача сигналу;

$P_{пер}$ – потужність передавача сигналу;

$G_{пер}$ – коефіцієнт спрямованої дії антени передавача сигналу;

$G_{пр\,з}$ – коефіцієнт спрямованого дії антени приймача-зловмисника;

$P_{пр\,з}$ – чутливість приймача-зловмисника;

FLS – втрати на відстані між передавачем сигналу та приймачем-зловмисником, пов'язані з умовами поширення сигналу;

$(S-N)_2$ – відношення сигнал/завада на вході приймача-зловмисника при заданих параметрах якості виявлення сигналу.

Для оцінки рівня енергетичної прихованості радіолінії в залежності від її параметрів і характеристик приймача зловмисника розглянемо більш детально структурну схему відвідного каналу в режимі перехоплення, наведену на рис. 1.

Будемо вважати, що ЦСПД працює зі швидкістю передачі інформації $R = 1/T$ (біт/сек), із заданим показником якості (із необхідною ймовірністю бітової помилки P_b) і при певному вигляді модуляції сигналу, що задає значення енергії сигналу на біт інформації E_b.

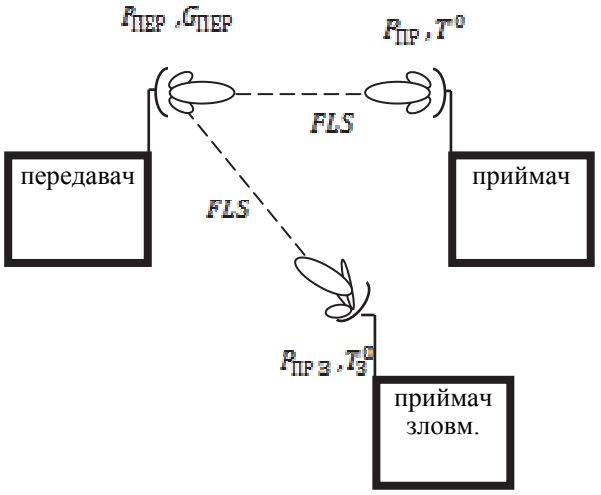

Рис. 1. Структурна схема відводного каналу (зловмисника) в режимі перехоплення

Тоді умова перехоплення сигналу може бути виражено нерівністю яку можна представити у вигляді декількох співмножників, що характеризують основні параметри каналу зв'язку:

$$\underbrace{\left(\frac{G_{пр}}{T^0}\right)}_{1} * \underbrace{\left(\frac{G_{пер}}{пер\,з}\right)}_{2} * \underbrace{\left(\frac{FLS_з}{FLS_ç}\right)}_{3} * \underbrace{\left(\frac{1}{SOM}\right)}_{4} * \underbrace{\left[\frac{1}{\left(\frac{2E_b}{N_0}\right)\frac{1}{T}*\left(\frac{T_i}{F}\right)}\right]}_{5} \le \underbrace{\left[\frac{G_{пр\,з}}{T_З^0 * Z_в}\right]}_{6}, \quad (4)$$

де 1 – характеристики приймача ЦСПІ: $G_{пр}$ – коефіцієнт спрямованої дії антени приймача і T^0 – шумова температура приймача;

2 – характеристики передавальної антени ЦСПІ: $G_{пер}$ – коефіцієнт спрямованої дії антени передавача і $G_{пер\,з}$ – коефіцієнт спрямованої дії антени передавача у напрямку до приймача-зловмисника;

3 – втрати в лінії зв'язку: – для легітимного каналу і $FLS_ç$ – каналу зловмисника;

4 – коефіцієнт запасу по потужності – SOM. Залежності відстані радіосигналу від чутливості приймача для різних значень параметру SOM представлені на рис. 2;

5 – коефіцієнт визначає параметри модуляції і широкосмуговості сигналу;

E_b – енергія сигналу на біт інформації;

N_o – спектральна щільність шуму;

F*T=B – база сигналу;

T_i – час інтегрування сигналу в приймачі-детектора.

6 – параметри приймача-детектора, що характеризують його технічну досконаліть і небезпеку перехоплення: $G_{пр\,з}$ – коефіцієнт спрямованої дії антени приймача-зловмисника; $T_з^0$ – шумова температура приймача-детектора; $Z_в$ – поріг виявлення.

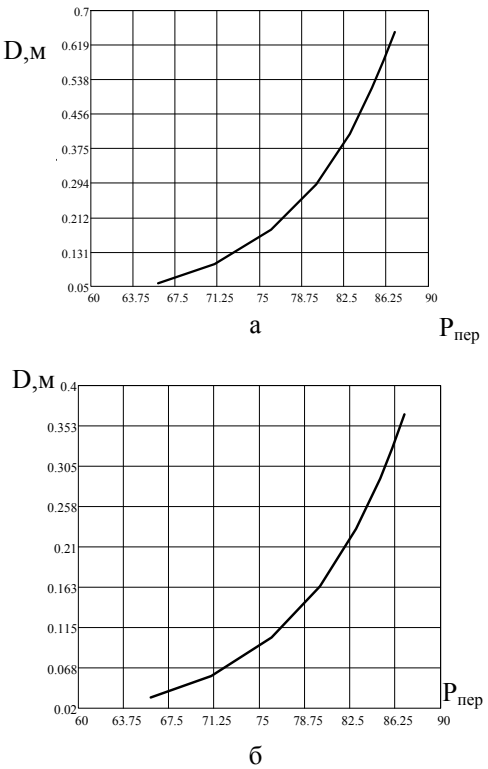

Рис. 2. Залежність відстані радіосигналу від чутливості приймача:
а – при запасі по енергетиці 15 дБ;
б – при запасі по енергетиці 20 дБ

Висновок

На підставі виразу (4) ми можемо стверджувати що для збільшення енергетичної прихованості легітимного каналу зв'язку, тобто зменшення відносини сигнал/завада на виході лінійної частини передавача, необхідно:

– використовувати в каналі спрямовані антени з мінімально можливим рівнем бічних пелюсток;

– використовувати приймач з малим рівнем власних шумів;

– втрати на поширення електромагнітної енергії сигналу на трасі легітимного каналу повинні бути значно менше, ніж втрати на трасі порушника $FLS_{\pi} << FLS_{c}$);

– використовувати в якості несучого сигналу складні сигнали з найбільшим значенням бази $(B_{c} << 1)$.

Список літератури

1. Lian, S. Multimedia Content Encryption: Techniques and Applications [Текст] / S. Lian. – CRC: Taylor&Francis, 2009. – 217 p.

2. Мао В. Современная криптография. Теория и практика [Текст] / В. Мао. – М.: ИД Вильямс, 2005. – 768 с.

3. Leung-Yan-Cheong, S.The Gaussian wire-tapchannel [Текст] / S. Leung-Yan-Cheong, M.E. Hellman // Information Theory, IEEE Transactions. – 1978. – № 4. – P. 451-456.

4. Методы прогнозирования защищенности ведомственных систем связи на основе концепции от водного канала [Текст]: моногр. / В.Г. Лихограй, А.А. Стрельницкий, А.Е. Стрельницкий, А.И. Цопа, В.М. Шокало; под ред. А.И. Цопы, В.М. Шокало. – Х.: КП Городскаятипография, 2011. – 501 с.

5. Хорошко, В. А. Методы и средства защиты информации [Текст]: учеб. пособ. / В.А. Хорошко, А.А. Чекатков. – К.: ЮНИОР, 2003. – 504 с.

Надійшла до редколегії 12.06.2017

Рецензент: д-р військ. наук проф. Г.А. Дробаха, Національний університет Повітряних Сил ім. І. Кожедуба, Харків.

ПУТИ УВЕЛИЧЕНИЯ ЭНЕРГЕТИЧЕСКОЙ СКРЫТНОСТИ РАДИОКАНАЛА СТАНДАРТА IEEE 802.11ИТС ГОСУДАРСТВЕННОЙ ПОГРАНИЧНОЙ СЛУЖБЫ УКРАИНЫ

Д.А. Волынец

В условиях активного внедрения в оперативно-служебную деятельность правоохранительных подразделений мобильных средств доступа к ведомственным информационным структурам, значительным увеличением использования мобильных радиотерминалов та сетевого радиооборудования, встает вопрос обеспечения безопасности использования беспроводных каналов.

В исследовании, на основе модели перехвата радиосигнала, с целью достижения максимального уровня энергетической скрытности, формируются требования к радиосистеме стандарта IEEE 802.11 пограничного подразделения.

Ключевые слова: *Гарт, АРМ, модель открытых систем, энергетическая скрытность, Wi-Fi канал, скрытность информации, вероятность выявления сигнала, структура сигнала, сигнал/шум.*

WAYS TO INCREASE THE ENERGY SECRECY OF A RADIO CHANNEL OF THE IEEE 802.11ITS STANDARD OF THE STATE BORDER SERVICE OF UKRAINE

D. Volinets

In conditions of active introduction into the operational-service activity of law enforcement units of mobile means of access to departmental information structures, a significant increase in the use of mobile radio terminals and network radio equipment, the issue of ensuring the safety of using wireless channels arises.

In the study, based on the radio signal interception model, in order to achieve the maximum level of energy secrecy, requirements are formulated for the radio system of the IEEE 802.11 standard of the border guard unit.

Keywords: *Garth, open systems model, power concealment, Wi-Fi channel, information concealment, probability of signal detection, signal structure, signal/noise.*