УДК 621.391

Ю. П. Белокурський, О. Ю. Іохов, В. Є. Козлов, О. О. Щербина

ОРГАНІЗАЦІЯ ЗАХИСТУ КАНАЛІВ РАДІОЗВ'ЯЗКУ ПІДРОЗДІЛІВ ОХОРОНИ ПРАВОПОРЯДКУ УКРАЇНИ

Розглянуто питання організації захисту інформації, що циркулює в контурі управління підрозділу охорони правопорядку України, за принципом розумної достатності.

К л ю ч о в і с л о в а: радіозв'язок, захист інформації.

Постановка проблеми та аналіз публікацій. Для управління підрозділами охорони правопорядку (ПОП) України в місцях постійної дислокації, в ході здійснення маршів, при виконанні всіх видів службово-бойових завдань необхідні надійний радіозв'язок та захист інформації в каналах зв'язку. Існуючі розпорядчі та нормативні документи [1, 2] розглядають об'єкт захисту (ОЗ) з постійним складом і місцем розміщення, а це фактично відповідає умовам так званого "кампуса". Прикладом такого кампуса є військове містечко – місце постійної дислокації підрозділу з незмінними рельєфом місцевості, площею, розміщенням споруд, обладнанням системи захисту. Під час виконання завдань службово-бойової діяльності (СБД) ПОП рельєф, площа та інші складові елементи ОЗ можуть змінюватися у часі. При цьому незмінною залишається модель загроз – заглушування каналів зв'язку, перехоплення та/або підміна інформації. Важливим фактором, що потребує особливої уваги, стає швидке зростання кваліфікації і можливостей потенційних порушників щодо використання сучасних засобів розвідки, розкриття і протидії зв'язку. Це обумовлює актуальність даної публікації та її **мету** – розкрити принципи організації захисту інформації в каналах радіозв'язку ПОП України за умов розумної достатності.

Виклад основного матеріалу. Захист каналів радіозв'язку ПОП під час виконання всіх видів СБД вимагає достатньо великих матеріальних витрат, тому його доцільно реалізовувати за принципом розумної достатності [3], тобто з витратами, що є не більше мінімально потрібних. Головним при цьому є цінність інформації, необхідної для прийняття відповідних рішень.

Відомо, що інформація, особливо оперативна, з часом втрачає цінність, що можна в першому наближенні апроксимувати виразом [4]:

$$C(t) = C_0 \exp(-2{,}3\tau/\tau_{жц}),$$

де C_0 – цінність інформації у момент її появи; τ – час прийняття рішення (від моменту появи інформації до моменту її використання); $\tau_{жц}$ – тривалість життєвого циклу інформації (від моменту появи до моменту втрати актуальності).

На рис. 1 наведено залежність нормованої цінності інформації C від тривалості її життєвого циклу $\tau_{жц}$ за умови фіксованого часу прийняття рішення τ (час подано в умовних одиницях). При збільшенні τ від $0{,}1\tau_{жц}$ до $\tau_{жц}$ мінімальна необхідна часова стійкість захисту інформації складає приблизно 3, 11, 46, 87, 99, 100 % від тривалості життєвого циклу, що визначає відповідне зростання витрат на організацію захисту інформації.

Таким чином, основним напрямком підвищення ефективності організації системи захисту радіозв'язку (СЗР) за умови розумної достатності є зменшення часу прийняття управлінських рішень щодо реалізації всіх видів СБД на всіх рівнях підпорядкованості. Це вимагає на етапі проектування СЗР ПОП детального дослідження об'єкта захисту; удосконалення моделі порушника; визначення складу апаратури і обладнання; розроблення відповідних нормативних, розпорядчих та експлуатаційних документів тощо за умови модульної побудови системи захисту за принципом "від простого до складного". На етапі експлуатації СЗР необхідним є моніторинг науково-технічних

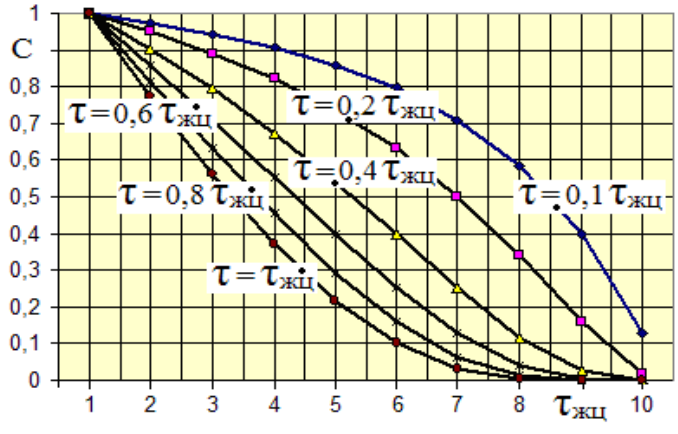


Рис. 1

досягнень в галузі засобів захисту (і нападу) з метою розвитку і модернізації системи. Такий підхід суттєво зменшить витрати на організацію захисту інформаційного обміну ПОП.

Створювати будь-які системи захисту інформації необхідно за міжнародними, національними, галузевими стандартами, рекомендаціями, методиками в галузях інформаційної безпеки, радіозв'язку, електромагнітної сумісності (ISO, IEC, ITU), Держспецзв'язку, Держспоживстандарту, Укрчастотнагляду. В межах правового поля система захисту для ПОП будується за моделлю системи радіоелектронної боротьби. Складові частини радіоелектронної боротьби – радіомаскування, радіопротидія і радіорозвідка.

Радіомаскування – комплекс організаційних і технічних заходів, що проводять з метою підвищення розвідзахищеності системи зв'язку.

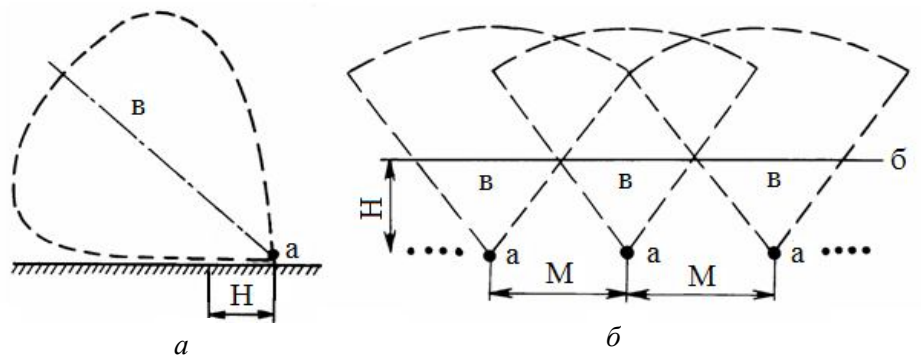
Організаційні заходи – створення фальшивих радіомереж (за планом вищого штабу) з імітацією роботи в них, як у реально діючих радіомережах і радіонапрямках; скорочення до мінімуму часу роботи радіозасобів на випромінювання; заборона використання засобів зв'язку посадовими особами і радистами з явно вираженими дефектами мови; управління військами за допомогою формалізованих документів, короткими сигналами і командами, з дотриманням вимог прихованого управління; виділення висококваліфікованих радіофахівців для роботи в найбільш важливих радіомережах (радіонапрямках); організація суворого контролю за дотриманням дисципліни зв'язку та вимог прихованого управління; забезпечення зв'язку проводовими засобами, коли це дозволяють умови обстановки (в районах зосередження військ, у місцях постійної дислокації).

До технічних заходів радіомаскування відносяться такі: робота радіозасобів із мінімально необхідною потужністю; застосування антен спрямованої дії; використання захисних (екрануючих) властивостей місцевості, будівель, місцевих предметів; настроювання радіозасобів без виходу в ефір (на еквіваленти антен); застосування апаратури засекречування; своєчасне усунення характерних ознак у роботі радіозасобів, обумовлених несправністю радіопередавальних пристроїв; ідентифікація голосів власних операторів за аудіопаспортами; визначення, пошук і нейтралізація (знищення) встановлених противником передавачів завад разової дії.

Для ПОП способи радіомаскування визначаються доступними заходами протидії радіорозвідці протиборчої сторони щодо виявлення та ідентифікації джерел випромінювання, визначення місця їх розташування та належності, перехоплення і дешифрування повідомлень. При цьому слід враховувати, що канали радіозв'язку ПОП створюються як штатними засобами, так і засобами Hi-Tech.

Радіопротидія може бути організована на принципах активного екранування системи зв'язку кампуса, заснованого на зменшенні відношення сигнал/шум для приймачів, що здійснюють спроби несанкціонованого доступу до циркулюючої інформації.

Зазвичай співвідношення сигнал/шум менше одиниці для гарантованого захисту при всіх ситуаціях забезпечують за рахунок того, що під час роботи системи радіозв'язку безперервно випромінюють за периметр системи і вгору шумові сигнали заглушування [5], як це показано для вертикальної (рис. 2, *а*) і горизонтальної (рис. 2, *б*) площин (для спрощення не показані задні і бокові пелюстки діаграм направленості). Шумові сигнали заглушування мають потужність більшу, ніж потужність робочих сигналів у системі радіозв'язку, і перекривають всю смугу частот, що використовується в системі. Така побудова системи захисту потребує використання антен направленої дії. Вимоги до антен визначають такі чинники: конструкція, функціональність, управляємість діаграми направленості, ширина смуги частот.



а *б*

Рис. 2

Відстань *H* передавачів *a* від периметра території кампуса сумісно з шириною головного пелюстка діаграм направленості антен *b* визначає максимальну відстань *M* між окремими передавачами вздовж периметра таким чином, щоб між діаграмами направленості не було щілин. Це забезпечить суцільну шумову завісу.

Власне, суцільну шумову завісу можна не створювати, а прикрити тільки ті точки перетинання периметра кампуса, які є продовженням каналів зв'язку.

Розроблюючи заходи захисту, необхідно враховувати питання забезпечення електромагнітної сумісності (ЕМС). Забезпечення умов ЕМС досягається: а) мінімізацією завад, які можуть бути створені засобам державних військових формувань, установ, радіозасобам цивільного призначення; б) виконанням чинних екологічних норм. У випадку захисту заглушуванням конфлікт з вимогами ЕМС не існує, якщо використовувати відомчі засоби професійного ультракороткохвилевого радіозв'язку.

З метою визначення можливості реалізації активного екрану захисту проведено експеримент у кампусі одного з вищих навчальних закладів Харкова з пеленгації завад і заглушування радіостанції UNF-діапазону, засобів мобільного зв'язку і безпроводового доступу в локальному об'ємі [6]. Для забезпечення ЕМС виміри у каналах GSM, 3G проводилися у позаробочий час, дія завад не виходила за межі кампуса вищого навчального закладу.

Застосовуване обладнання: приймач AR-5000; антени типу "хвильовий канал" діапазонів CDMA, GSM 900 (13 елементів), GSM 1800, 3G (25 елементів); серійний малопотужний джаммер і генератор завад. Коефіцієнти підсилення антен 18–21 дБ.

Для мінімізації впливу відбитих електромагнітних хвиль від стін будівель і збільшення захисного коефіцієнта антени застосовано металеві рефлектори.

Випробувались мобільні телефони Motorola і Nokia, радіостанції LPD.

Експеримент показав: ефект заглушування CDMA, GSM спостерігається на відстані до 60 м у напрямку осі антени; у зворотному напрямку на відстані 8 м зв'язок не порушується; загасання сигналів у разі площинного заглушування та наявності натовпу глибиною 20–30 м збільшується на 25–35 дБ; захист активним екраном у випадку площинного заглушування в діапазонах UNF потребує антен з високим захисним коефіцієнтом.

При виконанні службово-бойових завдань на місцевості (у тому числі, в умовах міста) як рухливі і адаптовні системи заглушування та перехоплення можна використовувати імпровізовані засоби [7], але це питання потребує подальшого дослідження і опрацювання.

Адаптація до змін умов під час виконання службових завдань потребує виконання завдань радіопланування, зокрема, розрахунків покриття та інтерференцій, перехоплення рухомих систем зв'язку, оптимізації розташування станцій заглушування, розрахунку мінімальної потужності систем заглушування тощо. Зазначені завдання виконує програмний виріб HTZ warfare [8]. Він призначений для збройних сил, органів внутрішніх справ, спецслужб і має допомогти в організації радіоелектронної боротьби, тактичної комунікації, управління радіочастотним спектром. Програмний виріб враховує будь-який тип сучасних мереж безпроводового зв'язку (радіорелейних, транкінгових, мікростільникових), потужності передавачів. Він також формує оперативну карту обстановки для прийняття рішення щодо виконання службових завдань. Результати розрахунків відображаються в 3D-форматі, що дозволяє уявити радіоелектронну обстановку у будь-якій точці об'єкта захисту. HTZ warfare використовує Український державний центр радіочастот.

Висновки

"Принцип розумної достатності" передбачає використання під час створення системи захисту інформаційних каналів радіозв'язку ПОП України в кампусі, а також використання при виконанні службово-бойових завдань на місцевості рухливих імпровізованих засобів заглушування і зв'язку та використання сучасних спеціальних програмних засобів для мінімізації ризиків можливого збитку від несанкціонованого втручання у радіообмін.

Список використаних джерел

1. Доктрина інформаційної безпеки України [Текст] : Указ Президента України від 8 липня 2009 р. № 514/2009 // Офіційний вісник України. – 2009. – № 52. – С. 7–58.

2. Наказ "Про введення в дію Настанови з організації зв'язку та автоматизованих систем управління внутрішніх військ МВС України" від 09.07.2010 р. № 307 [Копія] / МВС України. – К.

3. Что такое "принцип разумной достаточности"? [Электронный ресурс]. – Режим доступа : bolshoyvopros.ru. – Загл. с экрана.

4. Ценность информации [Электронный ресурс]. – Режим доступа : ofsky0.narod.ru. – Загл. с экрана.

5. Способ защиты информационного обмена в локальной системе радиосвязи [Электронный ресурс] : пат. № 2114513 Рос. Федерация : МПК (2006. 01) H04K3/00; опубл. 27.06.98. – Режим доступа : http://www.freepatent.ru. – Загл. с экрана.

6. Активний екран захисту каналів радіозв'язку підрозділів внутрішніх військ [Текст] / Ю. П. Белокурський, В. В. Лишенко, О. О. Щербина та ін. // Зб. тез доповідей V наук.-практ. конф. Акад. внутр. військ МВС України, Харків, 28 березня 2013 р. – Х. : Акад. ВВ МВС України, 2013. – С.103–105.

7. Захист інформації у каналах управління підрозділами внутрішніх військ МВС України [Текст] / Ю. П. Белокурський, О. М. Горбов, О. Ю. Іохов та ін. // Зб. наук. праць Акад. внутр. військ МВС України. – 2013. – Вип. 1 (21). – С. 63–65.

8. Програмний виріб HTZ warfare [Електронний ресурс]. – Режим доступу : nppgeoport.ru. – Назва з екрана.

Стаття надійшла до редакції 15.05.2014 р.