УДК 002:004.056.53

О. Ю. Іохов, В. В. Антонець, О. М. Горбов, І. В. Кузьминич, В. В. Овчаренко

ОСНОВНІ АСПЕКТИ РАДІОЕЛЕКТРОННОГО ЗАХИСТУ СИСТЕМИ РАДІОЗВ'ЯЗКУ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ВНУТРІШНІХ ВІЙСЬК МВС УКРАЇНИ ПІД ЧАС ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ В УМОВАХ МІСТА

Розглянуто основні проблемні питання забезпечення радіоелектронного захисту системи радіозв'язку внутрішніх військ МВС України. Визначено структуру та основні поняття радіоелектронного захисту. Обґрунтовано напрямки подальших наукових досліджень.

Ключові слова: *радіоелектронний захист, категорії порушника, система радіозв'язку, радіоелектронний вплив, радіоелектронна боротьба.*

Постановка проблеми. Сьогодні вплив на систему управління – це невід'ємна частина протиборства будь-якого масштабу, зокрема у правоохоронній діяльності. У зв'язку з цим важливим напрямком у сучасних конфліктах є протистояння радіоелектронних систем. На фоні бурхливого розвитку та запровадження у всі сфери діяльності суспільства сучасних інформаційних технологій, автоматизованих систем, глобальних телекомунікаційних мереж виникла сукупність принципово нових проблем у сфері захисту системи управління від дії радіоелектронних засобів та систем протилежної сторони.

Проблеми захисту системи радіозв'язку внутрішніх військ (ВВ) від радіоелектронного впливу виникли з низки причин. По-перше, значно поширились і спростились умови дії радіоелектронного впливу (РЕВ) на систему радіозв'язку системи управління внутрішніми військами всіма категоріями порушників [1; 2; 3]. По-друге, відрегульовані за часів СРСР адміністративно-командні механізми застосування широким колом осіб різноманітних радіоелектронних засобів на сьогодні не відповідають сучасним умовам і значною мірою втратили свою ефективність. По-третє, накладає свій відбиток специфіка виконання службово-бойових завдань (СБЗ) внутрішніми військами.

Зазначене вище суттєво підвищує вразливість системи радіозв'язку тактичної ланки управління внутрішніх військ (ТЛУ ВВ) МВС України і як наслідок може призвести до зриву управління. Таким чином, постає проблема захисту системи радіозв'язку ВВ від РЕВ [4].

Аналіз останніх досліджень і публікацій. Результати аналізу нормативно-правової бази та останніх наукових досліджень стосовно питань радіоелектронного захисту (РЕЗ) системи радіозв'язку правоохоронних органів виявили відсутність чіткого опису будь-яких заходів з цього приводу. Радіоелектронній захист систем радіозв'язку Збройних Сил (ЗС) України залишився на рівні вісімдесятих років і не враховує всіх особливостей службово-бойової діяльності ВВ у міських умовах [5]. Поряд із цим розвиток систем РЕЗ країн НАТО, Ізраїлю, Китайської Народної Республіки та Російської Федерації є пріоритетним у військовій та правоохоронній сферах, тому системи РЕЗ та радіоелектронної боротьби (РЕБ) указаних країн науково досліджуються і вдосконалюються [4]. Проте з огляду на таємність досліджень у сфері РЕЗ бракує доступних закордонних джерел інформації, які б висвітлювали особливості побудови систем захисту від РЕВ. Основні видання з теорії РЕБ, виконані такими відомими вченими, як С. А. Вакін, Л. Н. Шустов, А. І. Палій, В. А.. Вартанесян, Ю. М. Перунов, Д. Ван-Брант, висвітлюють загальні теоретичні питання із захисту інформаційних систем без урахування особливих умов їх застосування під час виконання СБЗ внутрішніми військами у міських умовах [5].

Мета статті – провести аналіз засобів РЕБ порушника та їх впливу на систему радіозв'язку ТЛУ внутрішніх військ МВС України під час виконання СБЗ в умовах міста; визначити уразливі місця системи радіозв'язку ВВ у разі дії на неї засобів РЕБ порушника; показати специфіку РЕЗ внутрішніх військ порівняно із ЗС України; визначити завдання, рекомендації та напрямки подальших досліджень щодо підвищення ефективності РЕЗ внутрішніх військ у міських умовах.

Виклад основного матеріалу. Для виконання всього спектра СБЗ, які покладені на

внутрішні війська за різних умов обстановки, органи управління повинні забезпечити стійке оперативне приховане управління частинами та підрозділами ВВ. Досягнення вказаних властивостей управління з урахуванням умов міста під час виконання службово-бойових завдань ВВ є можливим тільки у разі використання радіозасобів [5].

До переваг радіозасобів можна віднести те, що вони дозволяють встановлювати зв'язок на необхідній відстані у стислі терміни і на будь-якій місцевості, забезпечують автономність роботи, а також мають можливість передавання інформації одночасно великій кількості кореспондентів. Разом із цим радіозв'язок має і свої вразливі місця, зокрема:

– у процесі роботи не забезпечується прихованість передачі інформації;

– зв'язок може бути порушений радіозавадами;

– організований правопорушник, використовуючи радіопеленгатори, може визначити місце розгортання радіозасобу, а по ньому й пункт управління, і, відповідно, впливати на нього [4].

Це дозволяє порушникові вживати адекватні заходи ще на етапі прийняття рішення та передачі команд (розпоряджень) командирами і штабами частин та підрозділів внутрішніх військ МВС України, що надає йому інформаційну перевагу [2].

Як переконує досвід локальних конфліктів останнього десятиріччя, ескалація збройного конфлікту починається з дестабілізації політичного та економічного стану в одній із конфліктуючих сторін (наприклад, Лівія – 2011 р., Сирія – 2012 р.).

Для визначення можливості та характеру впливу на систему радіозв'язку ВВ під час виконання завдань за призначенням у міських умовах стисло розглянемо порушника, спроможного впливати на вразливі місця цієї системи. За нашою думкою, можна визначити три категорії порушника [6].

1. Організовані злочинні угруповання, які ставлять за мету досягнення економічної вигоди будь-яким шляхом і мають у своєму розпорядженні певний фінансовий потенціал.

2. Радикально-екстремістські (націоналістичні, релігійні) рухи нашої країни, які мають для досягнення політичних та інших цілей фінансову підтримку від політичних партій та закордонних "спонсорів", зацікавлених у нестабільності нашої держави.

3. Висококваліфіковані фахівці – це особи, які працюють на замовлення і займаються створенням проблем гуманітарного та політичного характеру, збудженням мас населення, штовхаючи їх до масових заворушень, що нерідко супроводжуються терористичними проявами.

Зважаючи на зазначені вище вразливі місця радіозв'язку та визначення порушника, надамо визначення таким поняттям.

Засоби радіоелектронного впливу на систему радіозв'язку ТЛУ ВВ МВС України (ЗРЕВ) – це комплекс засобів та дій порушника зі зриву (порушення) роботи або зниження ефективності бойового застосування підрозділами внутрішніх військ МВС України радіоелектронних систем і засобів шляхом впливу радіоелектронними завадами на їх приймальні пристрої.

Радіоелектронний захист системи радіозв'язку ТЛУ ВВ МВС України – це сукупність заходів та дій підрозділів ВВ МВС України щодо усунення або ослаблення впливу на свої радіоелектронні об'єкти засобів радіоелектронного впливу порушника, захисту від ненавмисних взаємних радіозавад, технічних засобів розвідки порушника та від засобів фізичного знищення.

Розглянемо стан системи радіозв'язку ТЛУ ВВ МВС України щодо її спроможності протистояти системі ЗРЕВ порушника.

За роки незалежності України технічне оснащення та модернізація системи радіозв'язку ВВ МВС України проводилися частково. Засоби автоматичного засекречування радіозасобів давно вичерпали встановлені терміни експлуатації, держава не має фінансової можливості виготовляти ключову документацію, апаратура засекречування забезпечує безпеку радіозв'язку тільки для стаціонарної мережі, тактична ланка управління взагалі лишилася без засобів захисту інформації. У разі закупівлі радіозасобів не враховується необхідність технічних засобів радіомаскування та скремблерів, подібні засоби радіозв'язку можливо придбати у вільному продажу. Для виконання СБЗ прийняті на озброєння і використовуються радіозасоби таких виробників, як ICOM, KENWOOD, MOTOROLA. Режими робіт цих засобів сумісні

з режимами, які використовують радіолюбителі та комерційні структури. Це дозволяє їх безперешкодне перехоплення, прослуховування та визначення всіх технічних характеристик.

Поряд із цим можливості ЗРЕВ, які можна вільно придбати широкому колу осіб, постійно вдосконалюються як закордонними, так і вітчизняними виробниками. Основний напрям удосконалення ЗРЕВ – це можливість їх довгострокового та прихованого застосування, а саме: мініатюризація, простота їх використання, швидкість оброблення перехопленої інформації, можливість їх передислокації та маскування, робота від різних енергетичних джерел та ін. [8]. Указані ЗРЕВ за своїми технічними характеристиками поступаються засобам радіоелектронної боротьби, які перебувають на озброєнні збройних сил провідних країн світу, але специфіка виконання завдань за призначенням в умовах міста дає порушникові певні переваги і робить ці ЗРЕВ навіть більш дієвими, ніж засоби РЕБ збройних сил.

Отже, виникає гостра необхідність захищати систему радіозв'язку ТЛУ ВВ МВС України від впливу ЗРЕВ усіх категорій наведених вище порушників.

Вирішення цієї проблеми є можливим кількома шляхами, і одним із них є використання радіоелектронних засобів РЕБ ЗС України. Результати аналізу можливостей радіоелектронних засобів РЕБ ЗС України показують, що під час виконання деяких завдань за призначенням ВВ МВС України ці засоби повністю задовольняють потреби ВВ. Водночас при діях ВВ МВС України у міських умовах використання радіоелектронних засобів РЕБ ЗС України викликає багато запитань.

Розглянемо суттєву відмінність системи радіозв'язку під час виконання СБЗ ВВ МВС України у місті, на відміну від подібної системи радіозвязку ЗС України. На рисунку 1 зображено розміщення засобів РЕБ у бойових порядках підрозділів ЗС України.

На наведеній схемі виразно зображено відстані, на яких діє підрозділ РЕБ ЗС України (глибина до 45 км, по фронту – 30 км). Усі засоби РЕБ, розміщені на автомобілях та бронетехніці, постійно маневрують. Керівними документами з організації зв'язку ЗС України визначені протидії ЗРЕВ противника.

Розглянемо особливості здійснення протидій ЗРЕВ під час виконання завдання з ліквідації масових заворушень (див. рис. 2), проводячи паралель з радіоелектронним протиборством

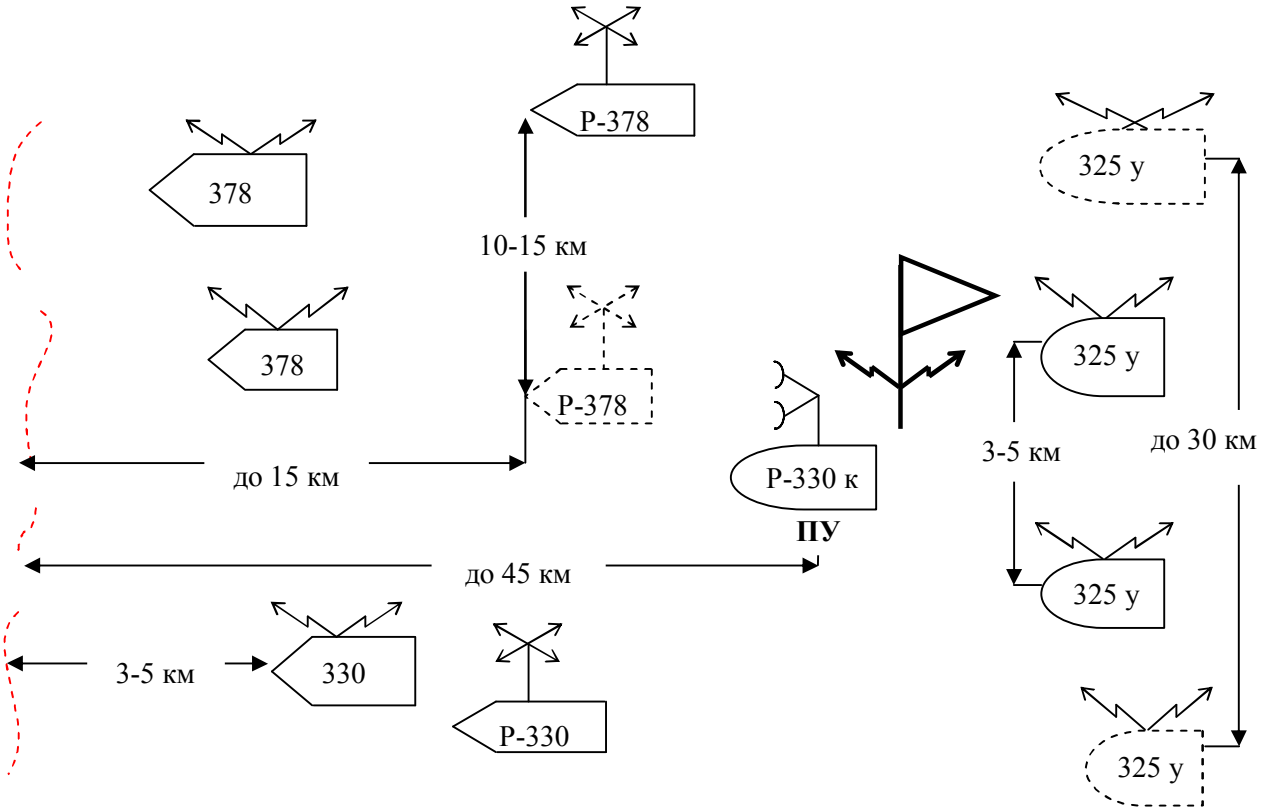

Рис. 1. Варіант розміщення засобів РЕБ у бойових порядках підрозділів ЗС України

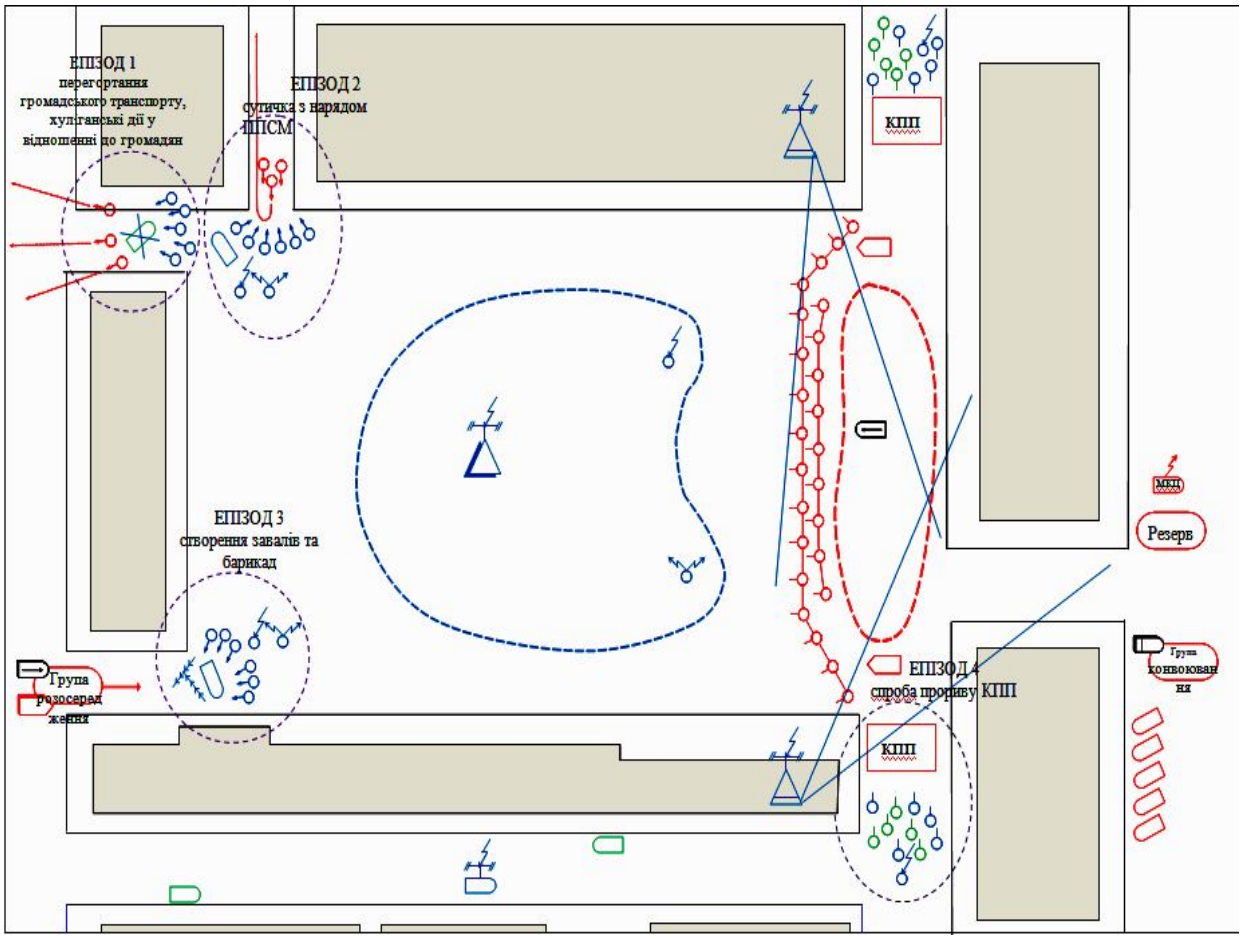

Рис. 2. Варіант застосування порушником засобів ЗРЕВ у різних умовах оперативної обстановки під час виконання СБЗ з ліквідації масових заворушень

противника в умовах ведення бойових дій ЗС України (див.рис. 1).

1. Фізичне знешкодження критично важливих елементів системи РЕБ противника. Сучасна нормативно-правова база України не дозволяє внутрішнім військам МВС України нейтралізувати порушників, які ведуть радіоелектронну протидію.

2. Порушення єдиного інформаційного простору противника. Порушник завжди володіє даними про місце розташування радіозасобів, частотний діапазон. Треба враховувати, що зазвичай порушник використовує засоби мобільного зв'язку загального користування, вимкнення яких під час масових заворушень може призвести до погіршення загальної обстановки.

3. Радіоелектронна дезінформація. З урахуванням оперативної обстановки під час виконання СБЗ ВВ МВС України у місті, а саме того факту, що порушник протягом проведення активної фази спеціальної операції з припинення масових заворушень має змогу спостерігати за діями підрозділів ВВ у реальному часі, виключаючи можливість прихованих дій, проведення заходів з радіоелектронної дезінформації не ефективне.

4. Маскування пунктів управління. Висота підйому антенних пристроїв візуально визначає місце розгортання засобів зв'язку та ЗРЕВ (див. рис. 3*а*). Розгортання засобів зв'язку та ЗРЕВ ЗС України, які базуються на вантажних автомобілях, у міських умовах [під час виконання СБЗ у міських умовах ВВ застосовують мобільний командний центр (МКЦ) на базі автомобіля "Газель"] ускладнено відсутністю достатньої площі для їх розгортання та організації охорони згідно з керівними документами (див. рис. 3*б*). Виникає загроза втрати цілком таємної апаратури та документації, з'являються труднощі в організації її охорони та виконанні режимних

а *б*

Рис. 3. Автоматизована станція перешкод УКХ радіозв'язку Р-330Т:
а – висота підйому щогли – 20 м; *б* – габаритні розміри 8600х2600х3845 мм

заходів [8]. Наявність у районі масових заворушень технічних засобів військового призначення, які будуть класифікуватися візуально як наявність військового складника, може призвести до провокаційних дій та дестабілізації оперативної обстановки. Порушник майже за всіх умов оперативної обстановки має можливість знаходитись у безпосередній близькості від бойових порядків ВВ, що дозволяє йому суттєво впливати на систему управління за допомогою стаціонарних (засоби, які встановлюються у будівлях в оперативному районі), пересувних (засоби, що встановлені на автомобілях) та переносних (рис. 4) ЗРЕВ. Порушник завжди володіє даними щодо місця знаходження радіозасобів та частотного діапазону, який використовується.

Таким чином, застосування тактики радіоелектронного протиборства противника в умовах ведення бойових дій ЗС України та використання засобів радіоелектронного протиборства ЗС України для виконання СБЗ внутрішніми військами МВС України неможливе.

Розглядаючи можливість використання засобів радіоелектронного протиборства СБУ, зазначимо, що відповідно до керівних настанов внутрішні війська МВС України виконують СБЗ у міських умовах у взаємодії зі СБУ [5]. Незважаючи на те, що підрозділи СБУ озброєні сучасними засобами радіоелектронної протидії, вони призначені для виконання виключно спеціальних завдань і мають обмежену кількість, тому не спроможні забезпечити підрозділи ВВ необхідними послугами РЕЗ.

Отже, сучасний стан систем радіозв'язку ТЛУ ВВ є критично вразливим і потребує підвищення рівня РЕЗ, що неможливо без додаткових технічних та наукових рішень [4].

Вирішення зазначеної проблеми можливе або за рахунок переобладнання новітніми комплексами радіозв'язку та системами радіоелектронного впливу (захисту), або шляхом модернізації існуючої системи радіозв'язку.

Яскравим прикладом у вирішенні таких проблемних питань є внутрішні війська МВС Російської Федерації. Зокрема, радіозасоби таких виробників, як ICOM, KENWOOD,

Дистанція придушення – до 300 м;
час безперервної роботи – до 8 год;
вага – 5…10 кг

Рис. 4. Пристрій придушення ліній радіозв'язку мобільних засобів "Вояж" 0918 (0819)

MOTOROLA, що перебувають на озброєнні частин та підрозділів внутрішніх військ МВС РФ, замінюються сімейством радіозасобів "Еріка" російського виробництва [6], яке розроблено виключно для забезпечення потреб внутрішніх військ.

У зв'язку з недостатністю фінансування повне переобладнання ВВ новітніми вітчизняними зразками неможливе. Радіоелектронні засоби (системи) РЕЗ розробляються науково-дослідними та виробничими об'єднаннями України для Служби безпеки та Збройних Сил України, проте, як згадано вище, вони не застосовуються для виконання СБЗ внутрішніми військами у міських умовах.

Альтернативою є використання закордонних засобів РЕЗ. Застосування цих засобів неможливе з певних причин: вони суперечать керівним настановам щодо розвитку та впровадження радіоелектронних засобів, можливості контролю режимів функціонування з боку держави виробника, а також щодо занадто великої вартості техніки та її обслуговування тощо [5].

Виходячи з наведеного вище на сучасному етапі розвитку внутрішніх військ єдиним шляхом забезпечення РЕЗ системи радіозв'язку ВВ МВС України є модернізація існуючих організаційно-технічних методів забезпечення РЕЗ цієї системи при мінімальних економічних витратах.

Результати аналізу методів побудови РЕЗ радіоелектронних систем дозволяють визначити загальну структуру та зміст РЕЗ системи радіозв'язку ТЛУ ВВ МВС України (рис. 5) [5].

Запропонована структура радіоелектронного захисту системи радіозв'язку ТЛУ ВВ МВС України потребує ввести такі визначення.

Інформаційно-аналітичне забезпечення РЕЗ ВВ МВС України – це функціонально

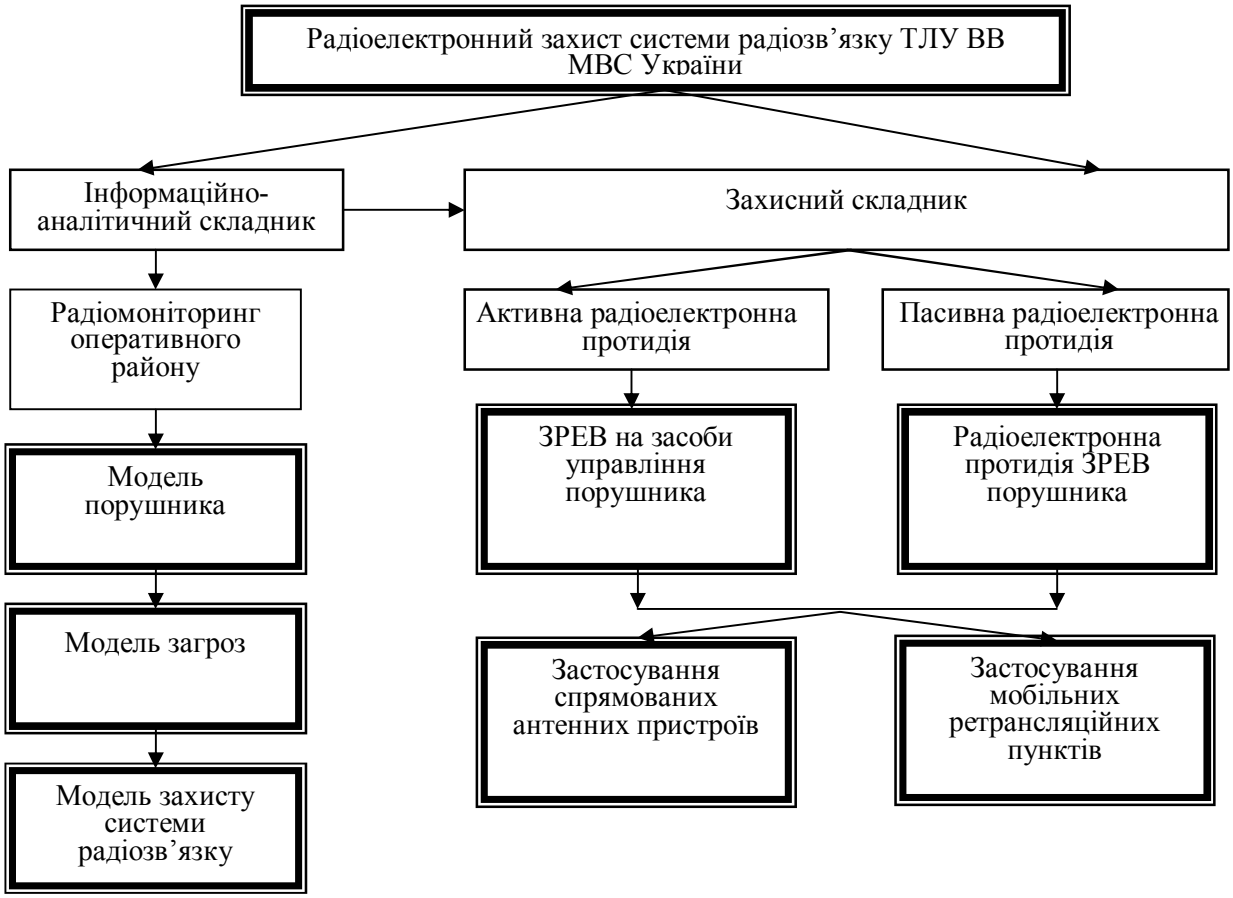

Рис. 5. Структура та зміст РЕЗ ВВ МВС України

закінчений інформаційно-технологічний комплекс організаційних структур, технічних, програмних і телекомунікаційних засобів, призначених для здійснення заходів з оперативного збирання, накопичення, оброблення, узагальнення і розповсюдження організаційно-технічної інформації РЕЗ ВВ МВС України.

Організаційно-технічна інформація РЕЗ ВВ МВС України – це сукупність організаційних, тактико-технічних вимог (профілі захисту) та перелік організаційно-технічних заходів для забезпечення РЕЗ ВВ МВС України.

Елементи інформаційно-аналітичного складника (ІАС) РЕЗ ВВ МВС України (див. рис. 5) на даному етапі побудови РЕЗ не визначені. Відомі методики, моделі та методи побудови ІАС не враховують особливостей використання системи радіозв'язку ВВ МВС України і мають розроблятися окремо.

Таким чином, на шляху побудови РЕЗ виникає необхідність вирішення низки науково-технічних завдань, пов'язаних з розробленням методики побудови профілю захисту системи радіозв'язку ТЛУ ВВ МВС України та основних складників цих профілів. Відповідно до цього побудова профілів захисту є можливою у разі отримання даних у процесі математичного моделювання порушника, загроз та визначення організаційно-технічної моделі РЕЗ системи радіозв'язку ВВ МВС України.

Захисний складник РЕЗ ВВ МВС України – це сукупність організаційних та технічних рішень, спрямованих на радіоелектронне знищення порушника, радіоелектронний захист своїх радіоелектронних об'єктів, а також радіоелектронно-інформаційне забезпечення системи управління ВВ МВС України.

Радіоелектронна протидія ЗРЕВ порушника – це сукупність заходів та дій щодо усунення або ослаблення ведення порушником технічної розвідки системи управління ТЛУ ВВ МВС України.

ЗРЕВ на засоби управління порушника – сукупність заходів та дій, спрямованих на радіоелектронне придушення засобів управління порушника, та засобів, які мають дистанційне радіокерування безпосередньо в оперативному районі виконання СБЗ підрозділами ВВ МВС України. Треба враховувати необхідність придушення технічної розвідки та систем управління порушника, у тому числі виключаючи можливість дистанційного керування вибуховими пристроями у безпосередній близькості від бойових порядків військ.

Розроблення і впровадження захисного складника РЕЗ ВВ МВС України визначаються за рахунок не тільки запровадження наукових новацій, але й економічної спроможності та можливостей зразків радіоелектронних засобів, які вже перебувають на озброєнні ВВ і є у достатній кількості. Зважаючи на ці обмеження, можна виділити прийнятні шляхи вирішення поставленої проблеми внаслідок використання малозатратних прихованих спрямованих антенних пристроїв та узгоджених з ними мобільних ретрансляційних пунктів. Мобільні ретрансляційні пункти перебувають на озброєнні ВВ і є у достатній кількості. Таким чином, виникає необхідність додаткових наукових досліджень, які полягають в удосконалюванні методів побудови камуфльованих (прихованих) спрямованих антенних пристроїв з урахуванням умов їх використання та показників існуючих засобів радіозв'язку ВВ МВС України.

Висновки

Сучасний стан радіоелектронних засобів ВВ МВС України та неможливість застосування внутрішніми військами засобів РЕБ Збройних Сил, Служби безпеки України, закордонних засобів робить систему радіозв'язку ВВ МВС України вразливою до дій радіоелектронних засобів впливу всіх категорій порушника.

Обґрунтованим шляхом забезпечення радіоелектронного захисту системи радіозв'язку ТЛУ ВВ МВС України є запропонована структура РЕЗ. Запровадження цієї структури РЕЗ потребує вирішення таких науково-технічних завдань, як: проведення моделювання порушника, загроз та визначення організаційно-технічної моделі РЕЗ для складання профілів захисту системи радіозв'язку ТЛУ ВВ МВС України; удосконалення методів розроблення і використання засобів радіоелектронного впливу на засоби управління порушника для захисту від радіокерованих пристроїв в оперативному районі виконання СБЗ внутрішніми військами МВС України в умовах міста; удосконалення методів побудови та використання камуфльованих (прихованих) спрямованих антенних пристроїв з урахуванням умов їх використання та умов тактико-технічних характеристик існуючих засобів радіозв'язку ВВ МВС України.

Список використаних джерел

1. Концепція технічного захисту інформації в Україні [Текст] : постанова Кабінету Міністрів України від 8 жовт. 1997 р. № 1126 // Уряд. кур'єр. – 1997. – 12 листоп. – С. 3.

2. Доктрина інформаційної безпеки України [Текст] : указ Президента України від 8 лип. 2009 р. № 514/2009 // Офіційний вісник України. – 2009. – № 52. – С. 7.

3. Хорев, А. А. Способы и средства защиты информации [Текст] / А. А. Хорев. – М. : МО РФ, 2000. – 316 с.

4. Визначення вимог до рухомих засобів зв'язку тактичної ланки управління внутрішніх військ МВС України при виконанні завдань за призначенням [Текст] : звіт про НДР / О. Ю. Іохов, І. В. Кузьминич, Г. А. Дробаха, М. М. Орлов, С. А. Горєлишев та ін. – Х., 2011. – 175 с. – № держреєстрації 0111U008896.

5. Розроблення рекомендацій щодо підвищення безпеки радіомереж тактичної ланки управління внутрішніх військ МВС України [Текст] : звіт про НДР / О. Ю. Іохов, О. М. Горбов, О. О. Казіміров, М. М. Орлов, І. М. Майборода, С. А. Горєлишев та ін. – Х., 2012. – 137 с. – № держреєстрації 0112U000529.

6. Ленков, С. В. Методы и средства защиты информации [Текст] : в 2 т. Т. I. Несанкционированное получение информации / С. В. Ленков, Д. А. Перегрудов, В. А. Хорошко; под ред. В. А. Хорошко. – К. : Арий, 2008.– 464 с.

7. Хорев, А. А. Классификация электронных устройств перехвата информации // Спецтехника и связь. – 2009. – № 1.– С. 46–49.

8. Про затвердження Настанови з організації зв'язку та автоматизованих систем управління внутрішніх військ МВС України [Текст] : наказ Міністерства внутрішніх справ України від 09.07.2010. р. № 307.

Стаття надійшла до редакції 14.12.2012 р.

Рецензент – доктор технічних наук, професор О. О. Морозов, Академія внутрішніх військ МВС України, Харків, Україна.