УДК 681.3

О. Ю. Іохов, О. М. Горбов

ОБҐРУНТУВАННЯ РОЗРОБЛЕННЯ МОДЕЛІ ПОРУШНИКА БЕЗПЕКИ ЗВ'ЯЗКУ У РАДІОМЕРЕЖАХ ВНУТРІШНІХ ВІЙСЬК ПІД ЧАС ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ

Запропоновано обґрунтування моделі порушника безпеки зв'язку у радіомережах внутрішніх військ МВС України.

К л ю ч о в і с л о в а: інформаційна безпека, модель порушника, система радіозв'язку.

Постановка проблеми. Аналіз безпеки систем радіозв'язку показує, що побудувати ефективну систему радіозв'язку неможливо без визначення моделі загроз для даної системи, яка безпосередньо ґрунтується на моделі порушника, що є її основою. Існуючі моделі порушника не здатні визначити весь потенціал його впливу на систему радіозв'язку внутрішніх військ під час виконання службово-бойових завдань. Виходячи з цього, виникає необхідність у розробленні моделі загроз для системи радіозв'язку внутрішніх військ МВС України під час виконання завдань за призначенням.

Аналіз публікацій. У сучасних наукових виданнях розглядаються різні методи складання моделі порушника у радіомережах, які базуються на моделюванні протидії промисловому шпіонажу та недобросовісній конкуренції (дані моделі ґрунтуються на виявленні порушень норм безпеки комерційних стандартів систем радіозв'язку Wi-Max, Wi-Fi, GSM, CDMA та ін., які на даному етапі не застосовуються у системі радіозв'язку внутрішніх військ). Моделі порушника, що розглядаються у системах радіозв'язку Збройних Сил України, розраховані на атаки підрозділів радіоелектронного придушення та засоби деструктивної дії (ядерна зброя, високоточна зброя). Отже, у ЗСУ передбачений захист від зазначених атак, який неможливо втілити у системі радіозв'язку внутрішніх військ.

Мета статті – обґрунтування розроблення моделі порушника системи радіозв'язку внутрішніх військ під час виконання всіх видів службово-бойових завдань, її всебічне оцінювання з урахуванням переходу засобів радіозв'язку внутрішніх військ на цифрові системи нового покоління.

Виклад основного матеріалу. В умовах сьогодення управління військами стає таким самим вирішальним фактором успіху виконання служба-бойових (бойових) завдань, як кількість військ і якість зброї, а співвідношення можливостей управління протиборчих сторін – не менш важливим показником, ніж співвідношення їх бойових сил і засобів. У сучасному бою та спеціальній операції, для яких характерні швидкі й різкі зміни обстановки, успішність дій військ напряму залежить від організованості цих дій, що безпосередньо визначається якістю управління. У досягненні потрібного рівня якості управління важливу роль відіграє зв'язок як процес доставлення повідомлень. Відомості, що містяться в повідомленнях, забезпечують знання обстановки, дозволяють виробляти рішення, ставити завдання військам (знову ж таки за допомогою передавання повідомлень) на виконання необхідних дій, спрямованих на досягнення мети службово-бойових завдань (бою).

Таким чином, простежується чіткий ланцюжок залежності, який виразно показує, що успішне виконання завдань системою зв'язку впливає на досягнення загальної мети службо-бойової діяльності (рис.).

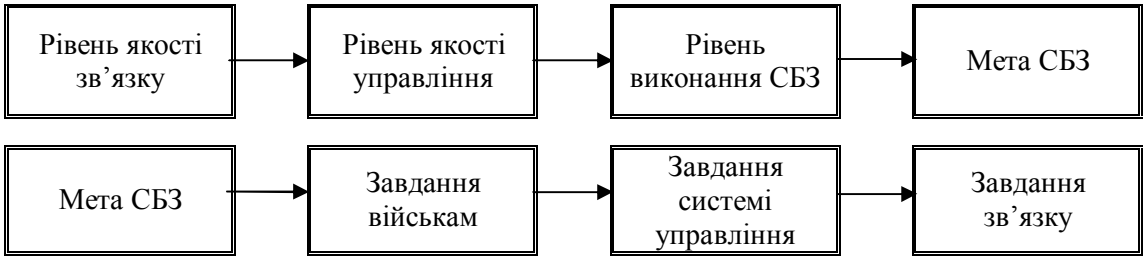

Рис. Залежність результатів службово-бойових завдань від якості зв'язку та визначення його завдань

Під час виконання внутрішніми військами завдань за призначенням основними технічними засобами управління є радіозасоби, які здатні забезпечити достатньо надійне управління частинами та підрозділами внутрішніх військ у будь-яких умовах обстановки. До переваг радіозасобів можна віднести те, що вони дозволяють встановлювати зв'язок у стислі строки практично на необхідну відстань і на будь-якій місцевості; автономність їх роботи; передавання інформації одночасно великій кількості кореспондентів. Разом з тим радіозв'язок має і свої недоліки [1]:

– у процесі роботи не забезпечується прихованість передавання інформації;

– зв'язок може бути порушений радіозавадами;

– організовані правопорушники (противник), використовуючи радіопеленгатори, можуть визначити місце розгортання радіозасобу, а відтак і пункт управління, але іншої альтернативи, ніж використання радіозасобів під час виконання внутрішніми військами завдань за призначенням, немає.

Жорсткість вимог до системи радіозв'язку на сучасному етапі обумовлена потребою органів управління в широкому спектрі послуг радіозв'язку, які забезпечують безперервне, стійке й приховане управління під час виконання службово-бойових завдань та реалізацію всього бойового потенціалу військ.

За роки незалежності технічне оснащення системи радіозв'язку внутрішніх військ МВС України проведено частково. Так, тривалість експлуатації засобів автоматичного засекречування радіозасобів перебільшує встановлені терміни, держава не має фінансової можливості виготовляти ключову документацію, апаратура засекречування забезпечує безпеку радіозв'язку тільки стаціонарної мережі, тактична ланка управління взагалі залишилась без засобів захисту інформації.

Навпаки, можливості технічних розвідок провідних країн світу та організованих злочинних угруповань постійно удосконалюються, апаратні потужності обчислювальної техніки для "злому" системи радіозв'язку збільшуються з кожним роком.

Досвід провідних країн світу із застосування систем радіозв'язку у локальних конфліктах показує, що радіозв'язок розвивається шляхом еволюційного впровадження новітніх телекомунікаційних технологій, систем цифрового та космічного зв'язку, які застосовуються у комерційних системах радіозв'язку для досягнення інформаційної переваги над противником. Під час аналізування систем радіозв'язку іноземних держав особлива увага зверталась на забезпечення безпеки систем оперативного радіозв'язку МВС Російської Федерації, яка має схожі завдання та характеристики з вітчизняною системою.

Внаслідок економічної нестабільності в Україні та недостатнього фінансування, у системі радіозв'язку внутрішніх військ не можливо реалізувати систему, подібну до аналогічних систем провідних країн світу. Отже, виникає гостра необхідність створення економічно ефективної, сучасної системи радіозв'язку, котра відповідатиме вимогам керівних документів із захисту інформації.

Виходячи з вищезазначеного, введемо поняття "інформаційна безпека радіозв'язку" та стисло розглянемо стан інформаційної безпеки радіозв'язку внутрішніх військ МВС України на сьогодні. Під інформаційною безпекою радіозв'язку внутрішніх військ розумітимемо захищеність інформації, що циркулює в системі, та здатність самої системи радіозв'язку протистояти навмисним або ненавмисним діям природного або штучного характеру, які можуть завдати значної шкоди системі управління внутрішніх військ.

Інформаційна безпека ґрунтується на забезпеченні конфіденційності, цілісності та доступності інформації, що циркулює у контурі управління. Доступ порушника до радіоканалу може призвести до перехоплення інформації, втрати контролю над системою захисту інформації, та "злому" самої системи захисту інформації. Кожна з цих загроз має свою специфіку для радіозв'язку і вимагає індивідуального вироблення механізмів їх усунення.

Аналіз загроз інформаційній безпеці радіозв'язку показує [2], що практично у всіх випадках (окрім ненавмисних завад) для порушення інформаційної безпеки системи радіозв'язку порушнику необхідна апріорна інформація про саму систему. Її можна отримати або агентурним шляхом, або за допомогою технічних засобів радіомоніторингу. Агентурний варіант блокується адміністративно-організаційними методами, потребує окремих досліджень у галузі захисту державної таємниці та розглядається окремо.

Зростання загроз для інформації, особливо в умовах інформаційного протиборства, яке набуває актуальності з кожним роком, вимагає розглядати захист інформації у системі радіозв'язку внутрішніх військ окремо від захисту інформації у проводовій мережі. З метою забезпечення захищеності інформації необхідно створювати більш дієві механізми захисту з урахуванням

вразливості системи радіозв'язку.

Для створення механізмів захисту безпеки системи радіозв'язку внутрішніх військ необхідно чітко визначити класифікацію порушників, які можуть діяти у ході виконання службо-бойових завдань внутрішніми військами, що надасть змогу забезпечити адекватний захист інформаційній безпеці системи радіозв'язку під час виконання завдань за призначенням.

Для класифікування порушників пропонується використовувати неформальну трирівневу модель [2]: *випадковий порушник* – хуліганські дії (низький рівень); *кваліфікований порушник*, який має певний програмно-апаратний комплекс (середній рівень); *висококваліфікований порушник*, який має засоби технічної розвідки та фінансове забезпечення (високій рівень). У таблиці наведено витяг із завдань, які виконують внутрішні війська за призначенням, та рівні порушників, які можуть пошкоджувати систему радіозв'язку. Проте дані питання потребують більш глибокого вивчення.

Таблиця

Витяг із завдань внутрішніх військ та рівні порушників, які можуть пошкоджувати систему радіозв'язку

Завдання ВВ (Закон про ВВ)	Завдання частин ВВ (накази, статути)	Види дій ВВ	Форми дій ВВ	Способи дій ВВ	Рівень порушника
Охорона та оборона важливих державних об'єктів, об'єктів матеріально-технічного та військового забезпечення МВС України	Охорона особливо важливих об'єктів державної власності, участь у фізичному захисті ядерних матеріалів і установок, перелік яких встановлюється Кабінетом Міністрів України	Охорона	Службово-бойові дії	Спостереження, затримання, супроводження	Середній
	Затримання, знешкодження терористів, які захопили ядерні енергетичні установки або ядерні матеріали	Спеціальні дії	Спеціальна операція	Блокування, пошук, оточення, прикриття, затримання, штурм, зачищення	Високий
	Відбиття нападу на об'єкт, що перебуває під охороною	Бойові дії	Бій	Перекриття шляхів руху діями із засад, затримання просування до об'єкта та знищення противника вогнем. Завзяте утримання рубежів на будь-якому напрямку дій противника, завдання йому поразки вогнем усіх сил і засобів	Високий
	Розшук і затримання порушників, які проникли на територію	Спеціальні дії	Спеціальна операція	Блокування, переслідування, розшук, пошук, оточення, затримання	Високий
	Розшук і затримання озброєних злочинців	Спеціальні дії	Спеціальна операція	Блокування, переслідування, розшук, пошук, оточення, затримання	Високий

Закінчення табл.

Завдання ВВ (Закон про ВВ)	Завдання частин ВВ (накази, статути)	Види дій ВВ	Форми дій ВВ	Способи дій ВВ	Рівень порушника
Охорона та оборона важливих державних об'єктів, об'єктів матеріально-технічного та військового забезпечення МВС України	Затримання, знешкодження злочинних груп, які захопили життєво важливі об'єкти на режимних територіях	Спеціальні дії	Спеціальна операція	Блокування, пошук, оточення, прикриття, затримання, штурм, зачищення	Високий
	Надання допомоги ОВС у пипинені групових і масових порушень громадського порядку на території охороняємого об'єкта, в охоронно-санітарних та населених пунктах, розташованих на режимних територіях	Спеціальні дії	Спеціальна операція	Оточення, охорона, розосередження, вилучення, патрулювання, конвоювання	Середній

Модель порушника системи радіозв'язку внутрішніх військ відображає можливі наслідки його дій (аналіз ризиків), має характер прогнозу і розробляється на основі накопиченого досвіду, але орієнтована на майбутнє. У процесі розроблення моделі порушника потрібно враховувати досвід інформативного протиборства у збройних локальних конфліктах, досвід протидії організованим злочинним угрупованням за останні 20 років, досвід захисту від хакерських атак на фінансові та інші об'єкти, факти промислового шпигунства, прогресивний розвиток мікропроцесорної, обчислювальної техніки та інші фактори.

Висновки

Модель порушника повинна відображати його практичні та теоретичні можливості, апріорні знання, фінансовий, технічний, ресурсний потенціал. У кожному випадку для системи радіозв'язку, що використовується у контурі управління, та конкретної обстановки потрібно визначати модель порушника для службово-бойових завдань, які виконують внутрішні війська. У процесі розроблення моделі порушника необхідно визначити:

– категорію осіб, до яких належить порушник;
– мотиви дій порушника;
– кваліфікацію порушника та його технічне оснащення;
– можливу мету порушника.

Отже, напрямком подальших досліджень може бути побудова моделі загроз системі радіозв'язку внутрішніх військ, підґрунтям якої є модель порушника для всіх завдань внутрішніх військ за призначенням.

Список використаних джерел

1. Кокотов, О. В. Модель загроз інформації в системах безпроводового зв'язку в умовах ведення інформаційної війни [Текст] / О. В. Кокотов. – К. : ВІТІ НТУУ "КПІ", 2009. – С. 3–18.

2. Григорьев, А. Н. Системы с защитой от несанкционированного доступа в конвенциональных радиосетях [Текст] / А. Н. Григорьев // Системы безопасности, связи и телекоммуникации: каталог. – 2003. – № 1(10). – С. 18–37.

Стаття надійшла до редакції 14.03.2012 р. .