УДК 551.510.42

О. М. Горбов, І. О. Радченко, К. В. Власов

МОДЕЛЬ ПОРУШНИКА ІНФОРМАЦІЙНОГО ОБМІНУ В РАДІОКАНАЛАХ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ

Розглянуто особливості побудови моделі порушника інформаційного обміну в радіоканалах сил охорони правопорядку під час виконання специфічних службово-бойових завдань. Визначені етапи побудови моделі порушника та її алгоритмізація.

К л ю ч о в і с л о в а : модель порушника, канал радіозв'язку, спеціальна операція.

Постановка проблеми. За роки незалежності України технічне переобладнання системи радіозв'язку тактичної ланки управління сил охорони правопорядку (СОПр) виконано частково. Засоби радіозв'язку військового парку фізично та морально застарілі і не відповідають вимогам технічної надійності. Засоби радіозв'язку міліцейського парку мають достатньо широку номенклатуру, яка задовольняє потреби системи тактичного радіозв'язку, але не повною мірою забезпечують захист інформаційного обміну, оскільки порушник активно впливає на розвідзахищеність, завадозахищеність та імітостійкість радіоканалів [1–3]. Засоби автоматичного засекречування засобів радіозв'язку військового парку вислужили встановленні терміни експлуатації, виникають труднощі з виробництва ключової документації, апаратура засекречування забезпечує безпеку радіозв'язку тільки стаціонарної мережі. Засоби радіозв'язку імпортного виробництва з функціями криптографічного захисту не відповідають вимогам керівних документів [4]. Досвід проведення антитерористичної операції у Донецькій та Луганський областях, виконання службово-бойових завдань (СБЗ) з припинення масових заворушень, антитерористичних операцій низки країн світу показує, що можливості технічних розвідок незаконних збройних формувань (НЗФ) та організованих злочинних угруповань постійно удосконалюються. Апаратні, програмні та технічні показники засобів радіоелектронної протидії (РЕПр) щодо впливу на системи радіозв'язку підвищуються з кожним роком. Вільне придбання, мініатюризація засобів РЕПр та простота використання надають можливість широкому колу осіб впливати на радіоканали СОПр під час виконання всього спектру СБЗ, які покладені на СОПр [2, 3].

Також звертаємо увагу на те, що застосування моделей та методів захисту радіоканалів, якими користуються Збройні Сили України, СБУ, силові структури інших країн, – неможливе [3].

Серед основних завдань, покладених на систему зв'язку СОПр, є такі: використання математичних моделей, методів і алгоритмів для накопичення, оброблення і ефективного пошуку інформації та надання її посадовим особам; моделювання можливих ситуацій, вирішення інформаційних, розрахункових та інших задач. На цей час система радіозв'язку підрозділів СОПр не враховує методи та моделі захисту інформаційного обміну.

Отже, інформаційний обмін у радіоканалах підрозділів СОПр є вразливим.

Аналіз останніх досліджень і публікацій. Обґрунтування створення моделі порушника інформаційного обміну в радіоканалах військового призначення наведено у статтях [2, 4]. Проаналізовано моделі порушника захищених корпоративних мереж зв'язку [5], технології забезпечення безпеки безпроводових мереж [5, 6], моделі атак порушника на підсистему криптографічного захисту у комп'ютерних системах [4]. Сьогодні, в умовах конкурентної боротьби у бізнесовій та фінансовій сферах, значна увага приділяється формуванню моделей порушника фінансової безпеки підприємства [6]. Постійно удосконалюються моделі порушника, який намагається проникнути на об'єкт, що охороняється [5].

Метою статті є удосконалення моделі порушника інформаційного обміну в радіоканалах шляхом сегментації використання радіоканалів для раціонального вибору засобів та заходів захисту радіоканалів підрозділів СОПр.

Виклад основного матеріалу. Планування зв'язку полягає у розробленні найбільш ефективних способів застосування сил і засобів зв'язку для забезпечення безперервного управління СОПр. Зв'язок планують на весь період виконання військами СБЗ. Одним з видів його планування є визначення заходів захисту елементів системи зв'язку від впливу засобів радіоелектронної боротьби організованих правопорушників (противника). Сучасні методики повною мірою не визначають моделі та методи захисту інформаційного обміну у радіоканалах СОПр від засобів радіоелектронної боротьби. Також варто зазначити, що існуючі організаційно-технічні заходи захисту інформаційного обміну у радіоканалах СОПр не є дієвими [2].

Порушник інформаційного обміну в радіоканалах СОПр – це угруповання, організація чи підрозділ, що зробили спробу виконання заборонених операцій (дій) усвідомлено, зловмисно, не

помилково та використовують для цього різні можливості, методи і засоби. Для радіоканалів підрозділів СОПр визначені такі категорії порушників [3]:

– організовані злочинні угруповання, які ставлять за мету досягнення певної вигоди будь-яким шляхом та мають у своєму розпорядженні певний фінансовий потенціал (перша категорія k_1);

– радикально-екстремістські (націоналістичні, релігійні, політичні) рухи України, метою яких є досягнення політичних та інших цілей; такі організації одержують фінансову підтримку від політичних партій і закордонних спонсорів, зацікавлених у нестабільності нашої держави (друга категорія k_2);

– наймані висококваліфіковані фахівці (або особи, які діють за їх завданням), мета яких – створення проблем гуманітарного та політичного характеру, збудження мас населення; вони "підштовхують" людей на заворушення, що нерідко супроводжуються терористичними проявами, призводять до загибелі великої кількості людей; порушник має можливість управляти заворушеннями, застосовуючи засоби РЕПр до радіоканалів правоохоронних органів (третя категорія k_3).

Наведені визначення загальні, вони не охоплюють всіх можливих порушників. Наприклад, дуже добре підготовлений порушник може застосовувати засоби радіоелектронного впливу з обмеженими характеристиками, а слабо підготовлений – засоби радіоелектронного впливу, характеристики яких близькі (в обмеженому районі) до характеристик засобів радіоелектронної боротьби військового призначення.

Модель порушника інформаційного обміну в радіоканалах підрозділів СОПр – це формалізований опис порушника, який визначає:

– категорії (типи) порушників, які можуть впливати на радіоканали підрозділів СОПР;

– вразливість сегмента застосування радіоканалів СОПр залежно від етапу проведення СБЗ або спеціальної операції (СО).

Розглянемо, чим відрізняється застосування відомих моделей від моделей порушника інформаційного обміну в радіоканалах підрозділів СОПр.

Модель порушника об'єкта, що охороняється. У даних типах моделей розглядаються такі характеристики порушника, як технічна, психологічна, фізична підготовленість, можливість подолання ним певних типів інженерно-технічних засобів охорони, швидкість пересування територією об'єкта та рівень інформованості про структуру системи охорони об'єкта. Сукупність цих характеристик дозволяє оцінити ймовірність проникнення порушника на об'єкт, а також сформулювати вимоги до інженерно-технічних засобів охорони і визначити сили та засоби підрозділів охорони. Загальними підходами до математичного опису формалізованої моделі порушника у даному випадку є ймовірнісний та детермінований. Кількісний опис параметрів порушника є складним завданням, на практиці найчастіше використовується комбінована модель, що поєднує елементи якісного і кількісного описів ймовірнісного і детермінованого підходів.

Модель фінансового порушника створюються з метою протидії промисловому шпіонажу та недобросовісній конкуренції. У даних моделях порушника можна виділити особу, яка здійснює спробу виконання заборонених операцій внаслідок помилки, незнання або свідомого використання для цього різноманітних можливостей, методів і засобів. Сукупність даних про елементи обличчя порушника дозволить адекватно зреагувати на можливі загрози та побудувати відповідну стратегію захисту фінансової безпеки підприємства. Сценарій розглядається як сукупність сцен порушення фінансової безпеки підприємства.

Модель порушника у телекомунікаційних мережах – це абстрактний (формалізований або не формалізований) опис порушника правил обмеження доступу. Такі моделі визначають категорії порушників, які діють на певні об'єкти телекомунікаційних мереж, а також мету, що переслідує порушник, його інструменти та приладдя, кількісний склад і т. ін., типові сценарії можливих дій порушника, способи його дій на кожному етапі. Дані математичні моделі є формалізованим описом сценаріїв у вигляді логіко-алгоритмічної послідовності дій порушника, кількісні значення яких параметрично характеризують результати таких дій.

Розглянуті підходи до моделювання не враховують вид СБЗ (СО), термін його виконання, зміни оперативної обстановки та визначають порушника як "внутрішній" або "зовнішній". Вихідні дані моделей розраховані на захист від порушника вищої категорії. Також не передбачене програмне моделювання зазначених моделей порушника.

Моделювання порушника радіоканалів Збройних Сил (ЗС) України та інших військових формувань не виконується через те, що порушник на полі бою завжди однієї категорії – це противник. Система захисту радіоканалів ЗС України розрахована на атаки підрозділів радіоелектронної боротьби противника та засобів деструктивної дії (ядерна зброя, ударні комплекси високоточної зброї та ін.). У ЗС України передбачений захист інформаційного обміну в радіоканалах

від таких атак залежно від виду та роду військ, який неможливо впровадити у систему радіозв'язку СОПр внаслідок низки причин [3].

При розгляді моделі порушника інформаційного обміну в радіоканалах силових відомств іноземних держав виникають об'єктивні труднощі через те, що інформація про такі моделі є обмеженого доступу. Також специфіка порушника, дії якого спрямовані проти нашої держави, та тактика дій підрозділів СОПр має свої унікальні характеристики.

У сучасних наукових виданнях моделі порушника радіоканалів (безпровідних технологій) комерційних стандартів (Wi-Max, Wi-Fi, GSM, CDMA та ін.) у процесі побудови захисту радіоканалів не розглядаються. Методи захисту зазначених стандартів ґрунтуються на використанні залежностей цінності інформації від криптографічного алгоритму, довжини ключа, алгоритмів аунтефікації, також у моделі враховуються заходи щодо недопущення сторонніх осіб у зону поширення інформативного радіосигналу [5]. Таким чином, розглянуті моделі та захист інформаційного обміну в радіоканалах не можуть бути ефективно застосовані у побудові захисту інформаційного обміну у радіоканалах підрозділів СОПр.

Модель порушника інформаційного обміну у радіоканалах підрозділів СОПр побудована на основі прогнозування рівня впливу порушника на сегмент застосування радіоканалів СОПр. Сутність методу полягає у визначенні залежності між категорію порушника та його впливом на кожен сегмент використання радіоканалу у конкретній оперативній обстановці. Дана залежність може бути застосована для підтримки прийняття рішення посадовою особою щодо раціонального застосування сил та засобів захисту радіоканалів. Структура методу складається з таких кроків:

– сегментація використання радіоканалів підрозділів СОПр залежно від виду та етапу проведення СБЗ (СО);

– присвоєння коефіцієнта ваги показникам вразливості радіоканалів для їх ранжирування;

– присвоєння рівня критичності кожному сегменту використання радіоканалів;

– алгоритмізація процесу визначення рівня впливу порушника на сегмент використання радіоканалів СОПР з метою автоматизації процесу.

Сегментація використання радіоканалів підрозділів СОПр залежно від виду та етапу проведення СБЗ (СО) виконується з визначенням завдання та його етапів (рис. 1).

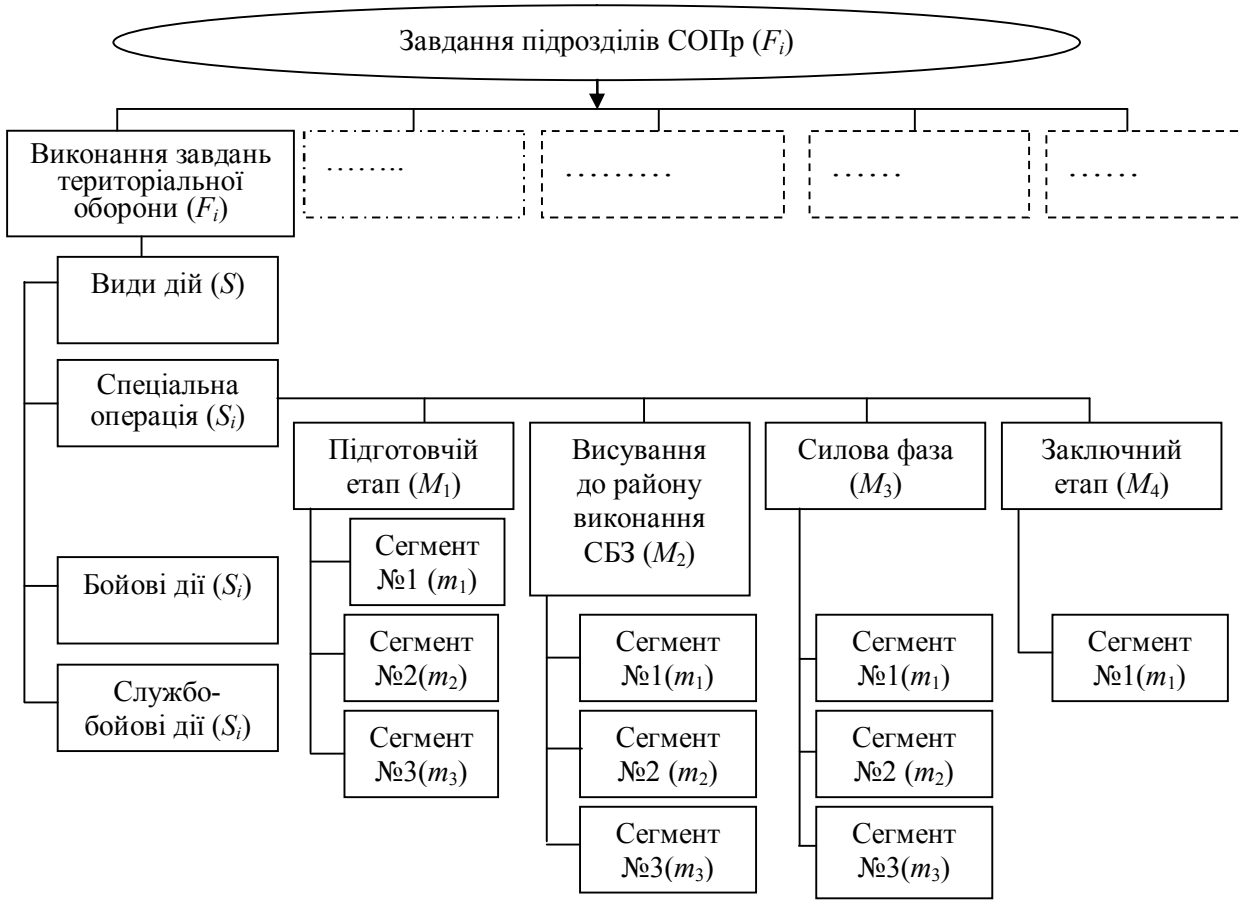

Рис. 1. Фрагмент сегментації використання радіоканалів підрозділів СОПр:
сегмент № 1 – радіомережі управління підрозділами СОПр; сегмент № 2 – радіомережі взаємодії;
сегмент № 3 – радіомережі стану

Сегментація використання радіоканалів також може здійснюватись шляхом визначення сегментів при проведенні всіх видів СО.

Присвоєння коефіцієнта ваги показникам вразливості радіоканалів для їх ранжирування та рівня критичності кожному сегменту використання радіоканалів розглянуті у статті [7].

З метою автоматизації процесу визначення ступеня впливу порушника на радіоканал здійснено математичний опис мовою предикатів, який дозволяє алгоритмізувати та програмувати процес вибору способу реалізації захисту інформаційного обміну в радіоканалі. Скористуємось логічними способами опису предметної галузі й подамо її мовою числення предикатів.

Позначимо через $M = \{m_i\}$ множину сегментів використання радіоканалу СОПр визначених СБЗ, потужність або кардинальне число якого дорівнює n [8, 9]. Кожний з елементів m_i цієї безлічі ($i = 1... n$) має деякий набір властивостей. Визначимо й подамо їх у вигляді набору вразливостей радіоканалу $B = \{b_j\}$, $j = 1… k$, а саме [9]: b_1 – радіорозвідка порушника (витік інформації), b_2 – радіоелектронний вплив (інформаційний вплив), b_3 – нав'язування хибної інформації (нестійкість), b_4 – деструктивний вплив (руйнація), та визначимо дані атрибути для кожної категорії порушника.

Теоретико-множинний запис: $m_i \in M$, його вразливість $m_i | B(m_i)$.

По суті кожен атрибут b_j являє собою деяку лінгвістичну змінну, яку можна оцінити за чотирибальною шкалою порядку експертним методом.

Будемо вважати, що граничним значенням оцінюваних нечітких величин є деяке число, наприклад, $\alpha \geq 4{,}00$, що у теорії нечітких множин називається α-зрізом функції належності. Інакше кажучи, вважатимемо, що при оцінюванні $m_i \in M$ того або іншого атрибута b_j значення величини $\alpha \geq 4{,}00$ показує, що радіоканал вразливий, а $\alpha < 4{,}00$ – не вразливий.

Уведемо подвійну індексацію величини α^i_j, де нижній індекс означає вразливість радіоканалу у переліку вразливостей, а верхній – номер сегмента. Особливістю процедури оцінювання таких нечітких атрибутів є те, що вони взаємозалежні та залежать від вразливості кожного сегмента радіоканалу.

Позначимо предикат $G(m_i(b_j))$, який означає, що деякий сегмент $m_i \in M$ має всі k вразливості $b_j \in B$, які можуть бути виміряні за чотирибальною шкалою. Тоді справедливі аксіоми, які визначають: радіоканал вразливий або не вразливий відповідно.

Аксіома 1. $\forall m_i G(m_i(b_1 \wedge b_2 \wedge b_3 \wedge b_4) \geq 4{,}00) \rightarrow 1$;

Аксіома 2. $\forall m_i G(m_i(b_1 \vee b_2 \vee b_3 \wedge b_4) < 4{,}00) \rightarrow 0$.

Наступним кроком методу є ранжирування вразливостей за ступенем їх впливу на радіоканал. Перша група способів, тобто тих, для яких справедлива аксіома 1. Для цього необхідно оцінити коефіцієнт відповідності – "сумарні" якості b_Σ тієї або іншої вразливості як згортку α^i_j [8] або чисельне значення функції належності [9].

У разі збігання таких оцінок окремих вразливостей на елементах безлічі утвориться квазіпорядок, наприклад, для трьох сегментів каналів радіозв'язку:

$m_1(b_\Sigma) = m_3(b_\Sigma) > m_2(b_\Sigma) = m_1(b_\Sigma) > m_4(b_\Sigma)$.

Остаточне ранжирування з урахуванням деяких додаткових умов буде подано у вигляді низки переваг:

$m_1(b_\Sigma) > m_3(b_\Sigma) > m_2(b_\Sigma) > m_4(b_\Sigma)$.

Тут знак ">" позначає відношення переваги.

Ранжированый список вразливостей радіоканалу: m_1; m_3; m_2; m_4.

Переходячи від аксіоматики до продукційних правил, які можуть бути використані в базі знань системи підтримки прийняття рішень, можна записати такі продукції.

1. Якщо з набору вимірюваних вразливостей $m_i | B(m_i)$ хоча б одна матиме значення $\alpha < 4{,}00$, то існує значний ризик того, що інформаційний обмін у радіоканалі буде зірваний.

2. Якщо з набору вимірюваних властивостей $m_i | B(m_i)$ всі вони мають значення $\alpha \geq 4{,}00$, то існує мінімальний ризик того, що інформаційний обмін у радіоканалі буде зірваний.

Запишемо предикати у такому вигляді.

Предикат 1. $\exists m_i \, \exists b_j G(m_i, b_1) \rightarrow 1$.

Предикат 2. $\exists m_i \, \exists b_j G(m_i, (b_1 \wedge b_2) \rightarrow 1$.

Предикат 3. $\exists m_i \, \exists b_j G(m_i, (b_1 \wedge b_2 \wedge b_3) \rightarrow 1$.

Предикат 4. $\exists m_i \, \exists b_j G(m_i, (b_1 \wedge b_2 \wedge b_3 \wedge b_4) \rightarrow 1$.

Наведемо змістовну інтерпретацію предикатів.

Предикат 1. Існує деякий сегмент застосування радіоканалу m_i, що має вразливість b_1. Цей предикат набуває значення 1, тобто це істина.

Предикат 2. Існує деякий сегмент застосування радіоканалу m_i, що має вразливості b_1 і b_2. Цей предикат набуває значення 1, тобто це істина.

Предикат 3. Існує деякий сегмент застосування радіоканалу m_i, що має вразливості b_1, b_2 і b_3. Цей предикат набуває значення 1, тобто це істина.

Предикат 4. Існує деякий сегмент застосування радіоканалу m_i, що має вразливості b_1, b_2, b_3 і b_4. Цей предикат набуває значення 1, тобто це істина.

Після підстановки конкретного сегмента радіоканалу, конкретної вразливості та її значення кожний з предикатів перетворюється у вислови.

Вислів 1. "Розвідзахищеність сегмента m_1 оцінена у 4,71 бала".

Вислів 2. "Розвідзахищеність сегмента m_1 оцінена у 4,71 бала, завадостійкість – у 4,86 бала".

Вислів 3. "Розвідзахищеність сегмента m_1 оцінена у 4,71 бала, завадостійкість – у 4,86 бала, імітостйкість – у 4,57 бала".

Вислів 4. "Розвідзахищеність сегмента m_1 оцінена у 4,71 бала, імітостйкість – у 4,86 бала, завадостійкість – у 4,57 бала, живучість – у 4,71 бала" .

Ряд переваг, ранжированый список і остаточні вислови для кожного сегмента радіоканалу подають особі, що приймає рішення, як висновок.

Визначення категорії порушника дає можливість раціонально використовувати засоби захисту інформаційного обміну (рис. 2).

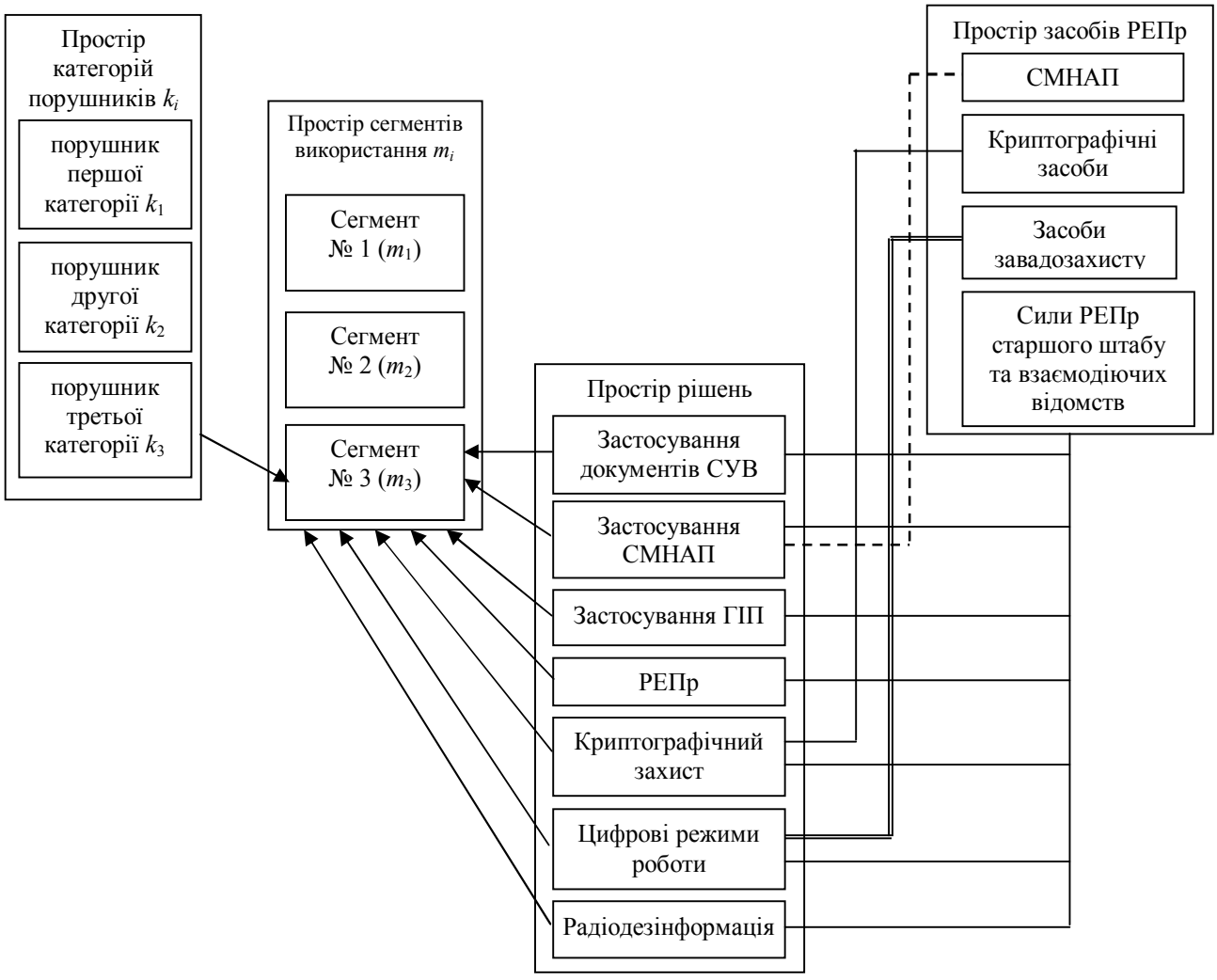

Рис. 2. Застосування засобів та заходів РЕПр до порушника третьої категорії:
СМНАП – скритний мобільний направлений антенний пристрій; ГІП – група інформаційної протидії

З рисунку видно, що, наприклад, для дієвого захисту радіоканалу від порушника третьої категорії необхідно використовувати всі можливі сили та засоби [10].

Висновки

Авторами удосконалена модель порушника, яка, на відміну від інших, використовує метод оцінювання рівня захисту сегмента застосування радіоканалів СОПр та дозволяє визначити залежність між категорію порушника і його впливом на кожен сегмент застосування радіоканалу під час виконання певного етапу СБЗ (СО).

Модель також дозволяє формалізувати можливості порушника щодо його впливу на інформаційний обмін у радіоканалах СОПр та дає змогу забезпечити раціональність вибору способу реалізації захисту інформаційного обміну в радіоканалах залежно від оперативної обстановки.

Використання мови предикатів дозволяє алгоритмізувати модель порушника інформаційного обміну в радіоканалах СОПр для підтримки прийняття рішення.

Список використаних джерел

1. Майборода, І. М. Особливості організації зв'язку під час проведення спеціальної операції по роззброєнню незаконних збройних формувань [Текст] / І. М. Майборода, К. В. Власов, О. М. Горбов // Честь і закон. – Х. : Акад. ВВ МВС України, 2010. – № 2. – С. 54–56.

2. Іохов, О. Ю. Обґрунтування розроблення моделі порушника безпеки зв'язку у радіомережах внутрішніх військ під час виконання завдань за призначенням [Текст] / О. Ю. Іохов, О. М. Горбов // Збірник наукових праць Академії ВВ МВС України. – Х. : Акад. ВВ МВС України, 2012. – Вип. 1 (19). – С. 31–34.

3. Основні аспекти радіоелектронного захисту системи радіозв'язку тактичної ланки управління внутрішніх військ МВС України під час виконання завдань за призначенням в умовах міста [Текст] / О. Ю. Іохов, В. В. Антонець, О. М. Горбов, І. В. Кузьминич, В. В. Овчаренко // Честь і закон. – Х. : Акад. ВВ МВС України, 2012. – № 4. – С. 40–47.

4. Кокотов, О. В. Модель загроз інформації в системах беспроводового зв'язку в умовах ведення інформаційної війни [Текст] / О. В. Кокотов. – К. : ВІТІ НТУУ "КПІ", 2009. – С. 28–57.

5. Кокотов, О. В. Модель порушника у телекомунікаційних мережах в умовах ведення інформаційної війни [Текст] / О. В. Кокотов, А. С. Шевченко // V наук.-практ. семінар "Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення", Київ, 3 вересня 2009 р. – К. : ВІТІ НТУУ "КПІ", 2009. – С. 140.

6. 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. 128–131.

7. Горбов, О. М. Метод оцінювання рівня захисту сегменту діяльності сил охорони правопорядку [Текст] / О. М. Горбов, В. Є. Козлов, О. О. Новикова // Системи обробки інформації. – Х. : ХУПС, 2015. – Вип. 2 (107). – С. 191–195.

8. Козлов, В. Є. Методика рейтингового оцінювання для експертного застосування [Текст] / В. Є. Козлов, В. Т. Оленченко, І. О. Юзьков // Системи управління, навігації та зв'язку. – Х. : ХУПС, 2009. – Вип. 4 (12). – С. 69–74.

9. Козлов, В. Є. Теоретико-множинний метод експертного оцінювання [Текст] / В. Є. Козлов, О. О. Новикова // Системи обробки інформації. – Х. : ХУПС, 2015. – Вип. 7 (132). – С. 291–293.

10. Настанова з організації зв'язку та автоматизованих систем управління внутрішніх військ МВС України [Текст] : наказ МВС України від 09.07.2010 р. № 307. – С. 1.

Стаття надійшла до редакції 29.05.2015 р.