УДК 621.396: 681.3.06

к.т.н. Міночкін А.І. (ВІТІ НТУУ “КПІ”)
д.т.н. Романюк В.А. (ВІТІ НТУУ “КПІ”)
к.т.н. Шаціло П.В. (СФ ВІТІ НТУУ “КПІ”)

ВИЯВЛЕННЯ АТАК У МОБІЛЬНИХ РАДІОМЕРЕЖАХ

Нове покоління мереж зв'язку 4*G* припускає використання мобільних радіомереж (МР) або MANET (Mobile Ad-Hoc Networks) [1, 2]. Зростаючий в останні роки підвищений науковий інтерес до дослідження МР обумовлюється появою недорогих бездротових мережевих рішень (стандарт IEEE 802.11, технології HiperLAN/2, Bluetooth). Класичним прикладом МР є перспективні мережі радіозв'язку тактичної ланки управління [3]. Виділимо особливості цих мереж: відсутність фіксованої інфраструктури (стаціонарних базових станцій); децентралізоване управління (кожен вузол автономний, виконує функції хоста та маршрутизатора); динамічна топологія (всі вузли мобільні); значна розмірність (сотні й тисячі вузлів); низька пропускна здатність радіоканалів (у порівнянні зі стаціонарними мережами); неоднорідність вузлів (по мобільності, ресурсам потужності й продуктивності); обмежена фізична безпека й ін.

Однією із завдань управління МР є забезпечення її безпеки [4–6]. *Метою статті* є аналіз: погроз безпеки, уразливості МР, потенційних атак супротивника й варіантів побудови ефективних систем їх виявлення.

1. Погрози безпеки та уразливості мобільних радіомереж

Атакою на інформаційну систему називається дія або послідовність зв'язаних між собою дій порушника, які приводять до реалізації *погрози* шляхом використання уразливостей цієї інформаційної системи [7].

Класифікація *погроз безпеки* в МР представлена на рис. 1. Прокоментуємо деякі з них. Погрози за метою впливу діляться на погрози порушення конфіденційності, цілісності й працездатності (доступності або відмови в обслуговуванні) [8]. Погроза порушення конфіденційності полягає в тім, що інформація стає відомою особам без відповідних повноважень доступу. Погроза цілісності містить у собі будь-яке навмисне перекручування (модифікацію або навіть видалення) інформації, що зберігаються у вузлах мережі або при її передачі по мережі. Погроза відмови в обслуговуванні виникає щораз, коли в результаті навмисних дій знижується продуктивність або блокується доступ до деякого ресурсу мережі або вузла.

Уразливості МР у порівнянні зі стаціонарними мережами визначаються особливостями її архітектури та протоколів функціонування [5, 6]:

1. Обмеженість фізичної безпеки радіоканалу. Широкомовна природа радіоканалу дозволяє супротивникові ставити активні й пасивні перешкоди, здійснювати прослуховування передач вузлів, аналізувати мережний трафік і розкривати існуючу систему управління військами.

2. Вузол може бути захоплений на поле бою супротивником або скомпрометований.

3. Динамічна топологія й колективна робота вузлів припускають уразливість функціонування протоколів канального, мережного й іншого рівнів, а також методів керування топологією, радіоресурсом і т.д. [4].

4. Обмеженість ресурсів елементів мережі: ємність батареї, обсяг пам'яті, продуктивність процесора вузла; пропускна здатність радіоканалу й ін.

Рис. 1. Класифікація погроз безпеки МР

2. Класифікація атак в мобільних радіомережах

Можна виділити наступні основні типи атак:

1. Аналіз мережного трафіка (з метою ідентифікації топології мережі, ідентифікації вузлів й їхньої ролі, ідентифікація протоколів обмела (маршрутизації, адресації й ін.), ідентифікація операційних систем, визначення вразливостей вузла й ін.).

2. Підміна довіреного об'єкта мережі.

3. Впровадження помилкового об'єкта мережі (наприклад, за допомогою помилкового маршруту) з подальшою селекцією (модифікацією) або підміні на ньому потоку інформації.

4. Відмова в обслуговуванні (насичення смуги пропущення, переповнення буферів й ін.).

5. Порушення прав доступу.

6. Завантаження ворожого змісту (модифікація інформації при її передачі по мережі або в процесі обробки та зберігання на вузлі, порушення конфіденційності інформації й ін.).

За аналогією із провідними мережами атаки залежно від характеру дій супротивника діляться на *активні* й *пасивні* (рис. 2). *Пасивні атаки* здійснюються шляхом несанкціонованого прослуховування радіоефіру й аналізу мережного трафіка. У цьому випадку атакуюча сторона не порушує нормальну роботу протоколів інформаційного обміну. Виявити пасивні атаки в бездротовому середовищі звичайно неможливо й відповідно захиститися від них досить складно. Відзначимо, що простір проведення пасивних атак обмежено зоною радіозв'язності.

Пасивні атаки відбуваються без впливу на процес передачі інформації, у той час як активні атаки включають перетворення, модифікацію й/або введення помилкової інформації (у тому числі й керуючої). Результат дій активних

атак може варіюватися від блокування окремих вузлів, зниження продуктивності мережі (або її ділянки) до повної дезорганізації її роботи. Головна відмінність активних атак від пасивних полягає в тім, що вони можуть бути виявлені. У свою чергу активні атаки діляться: на *зовнішні* (супротивник використовує власне встаткування, відсутність скомпрометованих вузлів) і *внутрішні* (наявність у мережі скомпрометованих або захоплених вузлів мережі).

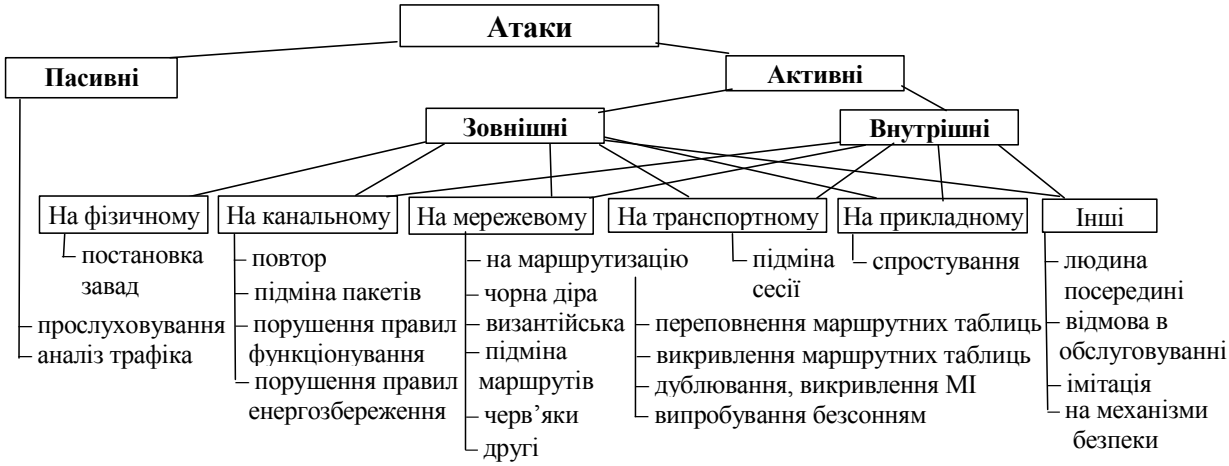

Рис. 2. Класифікація атак

Практично всі типи активних атак, що здійснюються у провідних мережах, можливі й у МР, наприклад, підміна сесії (hijacking), людина посередині (man-in-the-middle), нав'язування помилкового маршруту, повтор, руйнування маршрутів, відмова в обслуговуванні (DoS, Denial of Service), спростування (repudation), імітація (impersonation), затоплення (SYN Flooding) й ін. [8]. Хоча МР звичайно ізольована від загальної мережі (Інтернет), в той час атакуючий може використати її уразливості.

Реалізація активних атак у МР можлива на всіх рівнях еталонної моделі взаємодії відкритих систем (ЕМ ВВС).

На фізичному рівні супротивник може здійснювати постановку перешкод.

На канальному рівні атаки спрямовані на порушення правил функціонування протоколів канального рівня. Наприклад, використання децентралізованого канального протоколу IEEE 802.11 DCF (множинний доступ з контролем несучої) передбачає випадковий розиграш вікна *cw* (Contention Windows) початку передачі повідомлення [9]. Зловмисник може скористатися цим й, призначаючи мінімальне значення *cw*, одержувати пріоритетний доступ до каналу. Це приведе до значного зниження продуктивності в зоні радіопокриття супротивником. Крім цього, супротивник може порушити скоординовану роботу енергозберігаючих канальних протоколів [10], що приведе до якнайшвидшого виходу батарей вузлів з ладу. Атаки типу "повтор" (дублювання захоплених пакетів з метою накладення на передані пакети або створення помилкового трафіка) чи підміна (службових пакетів) також можуть значно знизити продуктивність радіоканалу.

На мережному рівні активні атаки спрямовані на протоколи маршрутизації [11]. Їх ціль – часткова або повна дезорганізація роботи МР шляхом введення в мережу повторної (застарілої) або помилкової (зміненої) маршрутної інформації (МІ): маршрутного повідомлення (для таблично-орієнтованих методів маршрутизації); зонда-запиту, зонда-відповіді, повідомлення про відмову маршруту при зондовій маршрутизації. Наприклад, атака типу "відмова в обслуговуванні" може бути легко реалізована модифікацією одного або декількох полів маршрутного повідомлення (зонда): адреси відправника (spoofing), числа ретрансляцій, номера повідомлення й самого маршруту передачі. Результатами активних атак можуть бути: перенапрямок маршрутів (і, відповідно, трафіка), зациклення маршрутів, створення перевантаження у вузлах мережі, переповнення маршрутних таблиць, імітація поділу мережі на окремі підмережі, збільшення часу доставки повідомлень і т.д.

Приведемо приклади деяких інших активних атак, які можуть бути здійснені в МР (рис. 1):

– "Чорна діра". У цьому випадку супротивник, використовуючи наявний протокол маршрутизації, повідомляє себе вузлом у найкоротшому шляху до адресата й переправляє весь трафік на себе.

– "Переповнення маршрутної таблиці". Супротивник прагне створити маршрути до неіснуючих вузлів. Ціль атаки полягає в створенні маршрутів, які б запобігли створенню нових маршрутів шляхом переповнення таблиці маршрутизації.

– "Випробування безсонням". Атака характерна для МР і спрямована на якнайшвидший розряд батарей вузлів. Супротивник може порушити функціонування енергозберігаючих протоколів різних рівнів ЕМ ВВС [10]. Крім того, генеруючи помилковий інформаційний й/або службовий трафік (наприклад, генеруючи зонди-запити на побудову маршруту до неіснуючих вузлів) ворог змушує вузли витрачати свою енергію батарей.

– "Виявлення місця розташування". Супротивник, використовуючи зондову маршрутизацію, розсилає зонди-запити [11]. На основі аналізу вмісту зондів-відповідей він намагається довідатися інформацію про місце розташування вузлів або розкрити структуру мережі.

– "Відмова в обслуговуванні". Атака спрямована на насичення ресурсу мережі (зв'язкового, обчислювального, по пам'яті) і може бути реалізована на будь-якому рівні ЕМ ВВС: на фізичному (постановка перешкод), на канальному (повторна передача, захоплення радіоканалу), на мережному (перенапрямок маршрутів) і ін. Вона також може бути спрямована на протоколи керування ключами [5].

Захист від зовнішніх атак включає застосування криптографічних методів: шифрування інформації, використання цифрового підпису й ін. [5]. Так цифровий підпис дозволяє перевірити дійсність, цілісність повідомлення, а також забезпечити його неспростовність (забезпечує захист від атак типу відмова, підміна й модифікація переданих даних). Для виявлення дублікатів пакетів і дотримання необхідного порядку їхнього надходження доцільно використати у форматі пакета тимчасові мітки й порядковий номер пакета. Однак,

криптографічні методи не можуть забезпечити захист від впливу супротивника при наявності скомпрометованих або захоплених вузлів. Для захисту від внутрішніх атак передбачається використати системи виявлення атак (СВА) або IDS (Intrusion Detection System) [6].

3. Класифікація систем виявлення атак

СВА можуть бути класифіковані [6, 11, 12] (рис. 3):

– за способом виявлення атаки – виявлення зловживань (процес виявлення атаки на основі порівняння поточного стану контрольованих ознак з апріорними відомостями про характеристики атак) і виявлення аномалій (процес виявлення атаки на основі порівняння дій користувачів із шаблонами нормальної активності);

– за об'єктом моніторингу – виявлення атак, спрямованих на всю мережу, окремий її сегмент (характерно для провідних мереж) або на конкретний вузол мережі;

– за прийняттям рішень – локальне й кооперовані (рішення про атаку приймається групою вузлів);

– за технологією прийняття рішень – використання технологій експертних систем, нейромереж, багатоагентних систем й ін.;

– за способом реакції на атаку – пасивні (реєструють атаку й повідомляють про її наявність) і активні (крім реєстрації й оповіщення перешкоджають зломщикові);

– за часом реакції на атаку – системи реального часу (on-line) і системи, що здійснюють періодичний аналіз ситуації (off-line).

Рис. 3. Класифікація систем виявлення атак

Виявлення аномалій припускає, що будь-які дії, що відрізняються від нормальних, інтерпретуються системою як атака. Це дозволяє виявляти атаки поза залежністю від апріорних знань про їх. Однак, така система не може самостійно (без втручання адміністратора) ідентифікувати атаку, отже, відсутня можливість автоматичної реалізації екстрених заходів щодо блокування атаки. Поряд із цим, істотним недоліком даного методу є потенційна можливість цілеспрямованого навчання системи зловмисником. Внаслідок цього атакуючі дії будуть розглядатися як нормальна активність суб'єкта. У зв'язку із труднощами реалізації в даний момент ця технологія не одержала широкого поши-

рення в комерційних системах. При настроюванні й експлуатації систем цієї категорії адміністратори зіштовхуються з наступними проблемами:

– побудова профілю користувача (важко формалізуєме й трудомістке завдання, що вимагає від адміністратора великої попередньої роботи).

– визначення граничних значень характеристик поводження користувача для зниження ймовірності появи одного із двох вищезгаданих крайніх випадків.

Виявлення зловживань полягає в описі атаки у вигляді шаблона (pattern) або сигнатури (signature) і пошуку даного шаблона в контрольованому просторі (мережевому трафіку або журналі реєстрації). Він дозволяє виявляти й ідентифікувати тільки атаки відомих типів. Підхід, реалізований у таких системах, дуже простий і саме на ньому засновані практично всі пропоновані сьогодні на ринку системи виявлення атак. Однак, адміністратори зіштовхуються із проблемами й при експлуатації цих систем. Перша проблема полягає в створенні механізму опису сигнатур, тобто мови опису атак. А друга проблема, що випливає з першої, як записати атаку, щоб зафіксувати всі можливі її модифікації. У той же час, при наявності в моделі механізму навчання можлива адаптація системи до розпізнавання нових типів атак.

Мережні (network-based) *СВА* аналізують мережний трафік реального часу на рівні окремих мережних пакетів і сесій на сегменті мережі (сукупності комутаторів, маршрутизаторів або шлюзів) з метою виявлення атак мережного рівня.

Вузлові СВА обробляють інформацію, що представляється у вигляді подій безпеки, які відбуваються під час функціонування вузлів мережі й змінюють їхні стани.

Принципова перевага мережних систем виявлення атак у тім, що вони ідентифікують напади перш, ніж вони досягнуть вузла, що атакує. Як правило, системи виявлення атак на рівні мережі працюють у реальному масштабі часу, у той час як системи, що функціонують на рівні хоста, забезпечують автономний аналіз реєстраційних журналів операційної системи або додатків.

За способом ухвалення рішення про наявність вторгнення СВА діляться на *локальні* (кожен вузол виявляє атаки й приймає рішення незалежно від інших вузлів) і *кооперовані*. Кооперене рішення про атаку може вироблятися між вузлами одного рівня – архітектура "автономний агент" (однорангова мережа) або вузлами різного рівня ієрархії МР (що характерно для тактичних МР) – архітектура "агент-менеджер".

Реалізовані СВА можуть бути на основі застосування технологій *експертних систем, нейромереж, багатоагентних систем й ін.*

Експертна система ґрунтується на наборі правил, які охоплюють знання людини – "експерта". На основі аналізу даних, одержуваних від модулів спостереження, експертна система робить висновок про стан об'єкта, що захищає. Експертні системи, використовуючи досвід, накопичений людиною, ідентифікують діяльність на відповідність сигнатурам (певним характеристикам зловживань або атак) [6]. Однак, експертні системи вимагають постійного відновлення для того, щоб залишатися актуальними. Системи на основі фіксованих

правил страждають від нездатності виявляти сценарії атак, які можуть мати місце протягом тривалих періодів часу.

Іншим перспективним підходом до реалізації СВА є використання нейронних мереж. Зміна природа мережевих атак вимагає гнучкої захисної системи, яка здатна аналізувати велику кількість мережевого трафіка способом, що є менш структурованим [6]. На відміну від експертних систем, які можуть дати користувачеві певну відповідь, відповідають чи ні розглянуті характеристики характеристикам, закладеним у базі правил, нейромережа проводить аналіз інформації й надає можливість оцінити, чи погодяться дані з характеристиками, які вона навчена розпізнавати. Якість визначення атаки безпосередньо залежить від реалізації нейромережі й від алгоритму її навчання. Важлива перевага нейромереж при виявленні атак полягає в здатності нейромереж "вивчати" характеристики навмисних атак (сигнатури) і ідентифікувати елементи (наприклад, трафік), які не схожі на ті, що спостерігалися в мережі колись.

Найбільш значний недолік застосування нейромереж для виявлення атак полягає в тім, що по своїй природі нейромережа представляє "чорний ящик" [6], тобто точність рішення часто є невідомою.

Третім перспективним підходом побудові комплексних систем захисту інформації (СЗІ), що дозволяє врахувати особливості функціонування МР, є технологія інтелектуальних багатоагентних систем [12]. Цей підхід дозволяє в порівнянні із традиційними методами істотно підвищити ефективність захисту інформації, у тому числі її адекватність, відмовостійкість, стійкість до деструктивних дій, універсальність, гнучкість і т.д.

Компоненти багатоагентної СЗІ (агенти захисту) являють собою інтелектуальні автономні програми, що реалізують певні функції захисту з метою забезпечення необхідного класу захищеності (рис. 3). Вони дозволяють реалізувати комплексну надбудову над механізмами безпеки використовуваних мережних програмних засобів, операційних систем і додатків, підвищуючи захищеність системи до необхідного рівня.

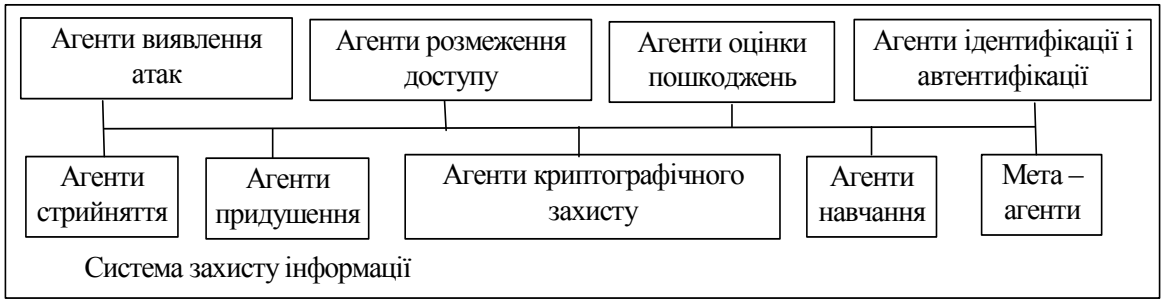

Рис. 3. Структура багатоагентної системи захисту інформації вузла мережі

Передбачається, що агенти розподілені по вузлах мережі, спеціалізовані по типах розв'язуваних завдань та взаємодіють один з одним з метою обміну інформацією й прийняття погоджених рішень. Важливо підкреслити, що в явному виді відсутній “центр управління” сімейством агентів – залежно від сформованої ситуації ведучим може ставати кожен з агентів, що спеціалізуються на завданнях керування. Якщо буде потреба, агенти можуть клонуватися й

припиняти своє функціонування. Залежно від ситуації (виду й кількості атак на МР, наявності обчислювальних ресурсів для виконання функцій захисту) може генеруватися кілька екземплярів агентів кожного класу. Вони адаптуються до реконфігурації мережі, зміні трафіка й новим видам атак, використовуючи накопичений досвід [12]. Виділяються наступні базові агенти: агенти сприйняття, агенти виявлення атак, агенти розмежування доступу, агенти ідентифікації й автентифікації, агенти придушення атакуючого, агенти оцінки ушкоджень і відновлення цілісності даних, агенти криптографічного захисту, агенти навчання, позначки-агенти.

4. Пропозиції по побудові СВА в мобільних радіомережах

Системи виявлення вторгнень, створені для провідних мереж не ефективні або не застосовні в МР. Виділимо основні розходження між бездротовою й стаціонарними СВА й, відповідно, пропозиції про побудові СВА в МР.

1. Тому, що трафік у радіомережі по своїй природі не може бути сконцентрований в одній точці, то мережева реалізація СВА не прийнятна для МР. Тому IDS-агент повинен бути активізованим на кожному вузлі МР і виконуватися незалежно (рис. 4).

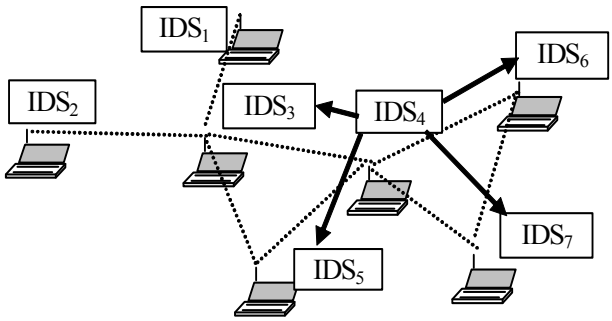

Рис. 4. Архітектура багатоагентної СВА для мобільних радіомереж

Варіант архітектури IDS-агента представлений на рис. 5. Вся поступаюча у вузол інформація проходить у реальному масштабі часу аудит і реєстрацію в модулі моніторингу й зберігається у відповідній базі даних. Модулі локального й кооперативного виявлення аналізують інформацію на предмет атак. Модуль безпеки здійснює криптографічні методи захисту при передачі службових повідомлень між IDS-агентами. Модулі реакції разом із системою управління мережею планують і здійснюють відповідні дії.

Реакцією на ідентифікацію або виявлення захоплених (скомпрометованих) вузлів може бути:

– виключення даних вузлів із процесу обміну інформацією (наприклад, побудова обхідних маршрутів) або їхнє придушення;

– зменшення впливу даних вузлів за рахунок передачі по декількох незалежних маршрутах передачі;

– зміна ключової інформації у вузлах мережі.

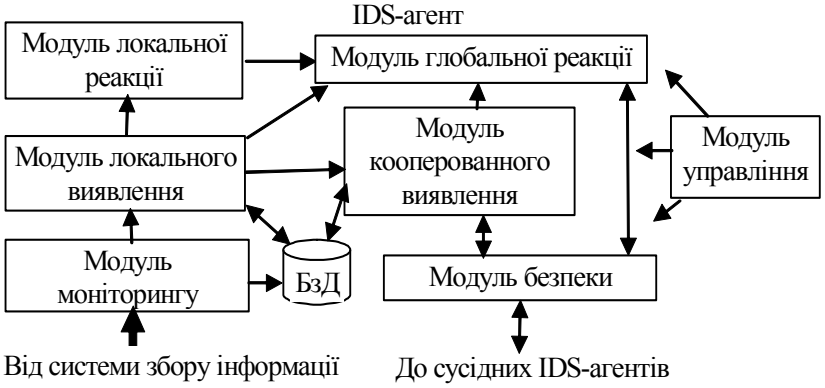

Рис. 5. Концептуальна модель IDS-агента

2. При кооперованій роботі СВА конкретний вузол не може повністю довіряти сусіднім вузлам, внаслідок можливої їхньої компрометації або захоплення.

Загальний підхід до аналізу поводження сусіднього вузла полягає в реалізації принципу “сторожового собаки” [14, 15]. Кожен вузол створює профілі нормального й аномального поводження сусіда по певних параметрах: мобільність, використовувані протоколи канального й мережного рівнів, частота перебудування або втрати маршруту, частота скидання пакетів, якість маршрутів тощо. За певний період часу здійснюється перерахунок контрольованих параметрів й уточнення ступеня довіри до сусіда. Остаточне рішення про компрометацію певного вузла може бути прийняте після узгодження свого ступеня довіри з іншими вузлами. Необхідно відзначити, що мобільність вузлів створює додаткові труднощі в розрізненні їх нормального й аномального функціонування.

3. Обмеженість ресурсів МР. Необхідність аналізу реального трафіка вимагає значної продуктивності комп'ютера, що входить у суперечність із наявними ресурсами вузлів МР. Тому реалізація багатоагентних СЗІ в повному обсязі функцій СВА можлива в мобільних базових станціях [2].

4. Виділимо основні вимоги до СВА в МР:

– децентралізованість функціонування;

– чутливість у певній області мережі (на відстані декількох ретрансляцій);

– низька величина помилкових спрацьовувань;

– мінімізація зв'язних й обчислювальних ресурсів;

– інтеграція модулів СВА на різних рівнях ЕМ ВВС і по функціях управління МР [4];

– наявність механізмів реакції на атаку.

Таким чином, захист від зовнішніх атак у МР повинен здійснюватися методами криптографічного захисту, внутрішніх атак – застосуванням систем виявлення атак. Проведений аналіз варіантів побудови СВА дозволяє зробити наступні рекомендації з їхньої побудови в МР:

– архітектура конкретної СВА буде визначатися архітектурою МР (для ієрархічних МР тактичного рівня доцільна архітектура "агент-менеджер");

– кожен вузол мережі повинен бути оснащений децентралізованої локальною СВА реального часу з можливістю колективного прийняття рішень по виявленню атак й відповідній реакції;

– перспективною технологією прийняття рішень у СВА є інтелектуальні мобільні агенти з використанням нейромереж і/або нечіткої логіки;

– функціонування СВА вузла повинне бути погоджене по рівнях ЕМ ВВС і функціях системи управління МР.

ЛІТЕРАТУРА

1. *Григорьев В.А., Лагутенко О.И., Распаев Ю.А.* Сети и системы радиодоступа. – М.: Эко-Трендз, 2005. – 384 с.

2. *Романюк В.А.* Мобильные радиосети – перспективы беспроводных технологий // Сети и телекоммуникации. – 2003. – № 12. – С. 62 – 68.

3. *Романюк В.А.* Напрямки розвитку тактичних систем зв'язку // II Науково-технічна конференція ВІТІ “Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”. – К.: ВІТІ НТУУ “КПІ”. – 2004. – С. 22 – 32.

4. *Миночкин А.И., Романюк В.А.* Методология оперативного управления мобильными радиосетями // Зв’язок. – 2005. – № 2. – С. 53 – 58.

5. *Міночкін А.І., Романюк В.А.* Безпека мобільних радіомереж // Збірник наукових праць № 5. – К.: ВІТІ НТУУ “КПІ”. – 2004. – С. 116 – 126 .

6. *Лукацкий А.В.* Обнаружение атак. – СПб: БХВ–Петербург, 2003. – 608 с.

7. *Максим М.*, *Полино Д.* Безопасность беспроводных сетей. – М.: ДМК Пресс, 2004. – 288 с.

8. *Медведовский И.Д., Семьянов П.В., Платонов В.В.* Атаки через Internet. – М.: НПО "Мир и семья", 1997.

9. *Миночкин А.И., Романюк В.А.* Методы множественного доступа в мобильных радиосетях // Зв’язок. – 2004. – № 2. – С. 46 – 50.

10. *Миночкин А.И., Романюк В.А.* Управление энергоресурсом мобильных радиосетей // Зв’язок. – 2004. – № 8.

11. *Миночкин А.И., Романюк В.А.* Протоколы маршрутизации в мобильных радиосетях // Зв’язок. – 2001. – №1. – С. 31 – 36.

12. *Zhang Y., Lee W.* Intrusion Detection in Wireless Ad-Hoc Networks // In Proceedings of IEEE MOBICOM, 2000. – pp. 275 – 283.

13. *Котенко И.В., Карсаев О.И.* Использование многоагентных технологий для компьютерной защиты информационных ресурсов в компьютерных сетях // Перспективные информационные технологии и интеллектуальные системы, 2001. – № 3.

14. *Marti S., Guuli T.J., Lai K., Baker M.* Mitigating Routing Misbehavior in Mobile Ad Hoc Networks // In Proceedings of IEEE MOBICOM, 2000.

15. *Huang Y., Lee W.* A Cooperative Intrusion Detection System for Ad Hoc Networks // In Proceedings of the ACM Workshop on Security of Ad hoc and Sensor Networks, 2003.