УДК 621.391

Сальник В.В. (ВІТІ)
Сальник С.В. (ВІТІ)
к.т.н. Бовда Е.М.(ВІТІ)
д.т.н. Сова О.Я. (ВІТІ)

АНАЛІЗ МЕТОДІВ НАВЧАННЯ БАЗ ЗНАНЬ ІНТЕЛЕКТУАЛЬНИХ ПІДСИСТЕМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В МОБІЛЬНИХ РАДІОМЕРЕЖАХ КЛАСУ MANET

Проведено аналіз існуючих методів навчання баз знань в інтелектуальних системах забезпечення безпеки мобільних радіомереж класу MANET. Здійснено класифікацію методів подання та отримання знань, які необхідно враховувати при побудові інтелектуальних систем забезпечення безпеки мобільних радіомереж класу MANET. Запропоновано напрямки побудови сучасних методів навчання баз знань інтелектуальних систем забезпечення безпеки у мобільних радіомережах. Також було визначено подальший напрям досліджень.

Сальник В.В., Сальник С.В., Бовда Э.Н., Сова О.Я. Анализ методов обучения баз знаний интеллектуальных подсистем обеспечения безопасности в мобильных радиосетях класса MANET. *Проведен анализ существующих методов обучения баз знаний в интеллектуальных системах обеспечения безопасности мобильных радиосетей класса MANET. Осуществлена классификация методов представления и получения знаний, которые необходимо учитывать при построении интеллектуальных систем обеспечения безопасности мобильных радиосетей класса MANET. Предложены направления построения современных методов обучения баз знаний интеллектуальных систем обеспечения безопасности в мобильных радиосетях. Также было определено направление дальнейших исследований.*

V. Salnyk, S. Salnyk, E. Bovda, O. Sova Analysis methods of teaching knowledge base of intelligent security subsystems in mobile radio networks class MANET. *The analysis of existing methods of teaching knowledge base in intelligent systems security class mobile radio networks MANET. Classification methods for submitting and obtaining knowledge that must be considered when building intelligent systems security class mobile radio networks MANET. Directions construction of modern methods of teaching knowledge base of intelligent security systems in mobile radio networks. It was also identified areas for further research.*

Ключові слова: *мобільна радіомережа, MANET, навчання баз знань, подання та отримання знань.*

Останнє десятиліття мобільні радіомережі (МР) класу MANET (Mobile Ad-Hoc Networks) стають все більш застосованими, як у повсякденному житті, так і у військовій галузі, а саме, в тактичній ланці управління військами [1]. Тому основним питанням під час побудови МР є забезпечення її безпеки. Актуальність вирішення цього питання пов'язана з характеристичними особливостями МР, такими як: передача інформації в радіосередовищі, динамічна топологія, масштабованість, що в свою чергу може бути використано противником для здійснення порушення безпеки МР.

Основною відмінністю МР від класичних радіомереж є відсутність фіксованої мережевої інфраструктури і, як наслідок, фіксованих маршрутів передачі інформації, що потребує використання принципово нових підходів до управління мережами даного класу.

Одним з таких підходів є використання децентралізованих систем управління (СУ) у складі кожного мобільного вузла [2], а також інтелектуалізація процесів управління МР [3]. Таким чином, МР повинна містити в собі підсистему управління безпеки (ПУБ), робота якої полягає в навчанні бази знань (БЗ) зі здатністю самонавчання [2].

Аналіз останніх досліджень і публікацій. Організація навчання баз знань в системах безпеки МР, захист мережі від вторгнень, а також питання проектування та побудови системи навчання баз знань в СЗБ розглядалися в роботах [1, 14 – 19].

Мета статті. Проведення аналізу існуючих методів навчання баз знань в інтелектуальних системах забезпечення безпеки в МР з метою визначення можливостей їх застосування в МР класу MANET.

Об`єкт розгляду статті. Процес отримання та подання знань в системі забезпечення безпеки про ситуацію в МР.

Предмет дослідження. Методи подання та отримання знань інтелектуальною системою забезпечення безпеки від протиправних дій противника в МР.

Виклад основного матеріалу. Система навчання баз знань (БЗ) в інтелектуальних системах забезпечення безпеки (ІСЗБ) МР, яка є складовою інтелектуальної системи управління має комплексний характер та включає теоретичну та практичну складові.

Інтелектуальної системи управління (ІСУ) в МР займає центральне місце в процесі обробки знань про стан вузлів і ситуацію, що склалася в МР. Управлінські рішення, які приймаються ІСУ, базуються на аналізі та оцінці великої кількості різнорідних параметрів функціонування вузлів та МР, встановити кількісну залежність між якими дуже важко або взагалі неможливо. Крім того, через постійні зміни умов функціонування МР, службова інформація про параметри функціонування вузлів дуже швидко старіє, є неточною і недостатньою для побудови чіткої математичної моделі функціонування МР. За таких умов в основу ІСУ повинна бути покладена система знань про об'єкти управління, в якості яких може виступати мобільний вузол, чи МР в цілому. Система знань повинна використовувати таку мову подання знань, яка б надавала можливості адекватно відтворювати структуру об'єктів управління і характеризувалася достатньою формальністю та логічністю з метою побудови строгої та компактної БЗ.

Аналіз сучасного стану досліджень. Навчання баз знань в інтелектуальних системах забезпечення безпеки (ІСЗБ) в МР являє собою складну динамічну систему зі здатністю обробки, отримання та подання знань в СЗБ в МР, яка здатна приймати управлінські рішення. При цьому варто звернути увагу на низку аспектів, які потрібно враховувати під час дослідження процесу збору знань в радіомережі класу MANET. Управління вузлом МР полягає в прийнятті рішень на вузлі, щодо забезпечення безпеки чи параметрів функціонування вузла, які забезпечать безпечну роботу вузла та мережі в цілому з урахуванням наявних вузлових та мережевих ресурсів [1, 4].

Ресурси, на основі яких здійснюється управління МР, зазначено на рис. 1.

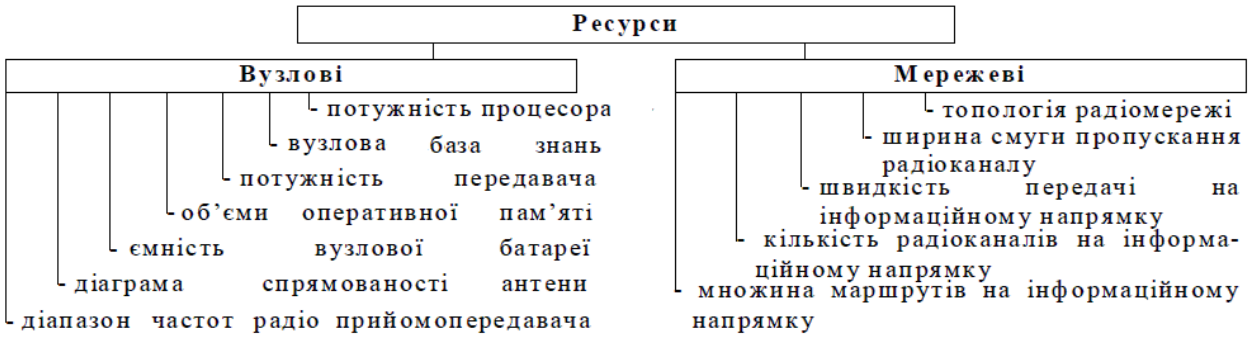

Рис. 1. Ресурси, на основі яких здійснюється управління МР

В МР кожен мобільний вузол наділений правами управління своїми ресурсами залежно від ситуації в МР та вимог до передачі того чи іншого типу трафіка в конкретний момент часу. Однак, з урахуванням того, що умови функціонування кожного мобільного вузла, так само як і їхні технічні характеристики, відрізнятимуться на етапах функціонування МР. Це означає, що під час проектування інтелектуальних систем забезпечення безпеки (ІСЗБ) потрібно передбачити розробку механізму координації управляючих рішень, які приймаються незалежно від моменту часу.

Виходячи з вищевказаного, функціонування будь-якої інтелектуальної системи ґрунтується на перетворенні інформації в знання, на основі яких приймаються управлінські рішення щодо ЗБ. ІСЗБ у результаті збору і обробки службової інформації отримує знання про стан інших вузлів і ситуації, що склалася в МР в цілому.

Ці знання являють собою сукупність відомостей про кожен вузол МР, а також множину правил використання цієї інформації для прийняття управлінських рішень в МР. На практиці оперування знаннями в будь-якій ІС здійснюється за допомогою бази знань.

Система забезпечення безпеки являє собою комплекс засобів щодо забезпечення захисту від загроз пов'язаних з можливістю втрати, перекручування та розкриття інформації (даних, ресурсу, тощо). Використання ІСЗБ актуальна для забезпечення безпеки в

інформаційних систем управління відкритого так і закритого типу мережі. Як зазначено в рис. 2 СЗБ включає наступні підсистеми: криптографічного захисту; забезпечення цілісності; аудиту; виявлення вторгнень; запобігання вторгнень; аутентифікації; оцінки ризиків; реагування; ідентифікації прогнозування та попередження.

Рис. 2. Підсистеми забезпечення безпеки

База знань ІСЗБ на вузлі МР – це особливого роду база даних, яка містить структуровану, подану в певній формі інформацію про стан МР, яка використовується для ЗБ та прийняття управлінських рішень на рівнях моделі OSI.

Основними особливостями вузлових баз знань (ВБЗ), які відрізняють їх від мережевих баз знань (БЗ) є здатність:

– формувати висновки в автоматичному режимі. БЗ повинна містити правила виводів, що дозволять вузловій ІСЗБ самостійно набувати нові знання на основі отриманих даних із середовища функціонування МР (самонавчання) [5];

– знаходити протиріччя, які можуть виникнути в ній самій;

– адаптуватися до нових умов функціонування мобільного вузла чи МР, що аналогічно здатності людини „отримувати досвід”.

Відповідно до вказаного, основну функцію БЗ, щодо обробки знань для забезпечення безпеки в МР можна розділити на дві складові: подання знань (знання можуть бути подані у вигляді текстів, формул чи графіків, ІСЗБ являє собою складну технічну систему, яка потребує апаратної та програмної реалізації), та отримання знань (постійне оновлення БЗ та поповнення її новими правилами, а також виключення людини з процесу управління вузловими та мережевими ресурсами) [6, 7].

У зв’язку з цим, розглянемо методи подання та отримання знань для визначення можливості їх застосування при розробці БЗ в ІСЗБ. Основні з них зображені на рис. 3 [1, 7], тому розглянемо їх детальніше.

Рис. 3. Методи подання та отримання знань в МР

Методи обробки знань Ґрунтується на перетворенні службової інформації в знання про ту чи іншу предметну область, на основі яких будуть прийматися управлінські рішення. ІСУ в МР у результаті збору і обробки службової інформації отримує знання про стан МР. Оперування знаннями в будь-якій ІСУ здійснюється базою знань.

Обробка знань досягається наступними методами: метод отримання знань; метод подання знань.

Отримання знань будь-якою ІСЗБ безпосередньо пов'язане з процесом її навчання, яке полягає в здатності ІСУ знаходити нові закономірності в інформації про предметну область та на їх основі створювати нові правила поведінки того чи іншого об'єкта управління. Основна ідея навчання ІС полягає в тому, що за наявності навчальної програми, а також навчальної вибірки може бути побудована певна модель закономірностей, що дозволить ІСЗБ знаходити закономірності в новій службовій інформації про стан вузла чи інформації в цілому про МР.

І. Методи отримання знань

Всі методи, які використовуються для навчання в сучасних підсистем забезпечення безпеки, можна поділити на два класи [6, 7]:

Дедуктивні методи – передбачають формалізацію знань експертів та їх перенесення в технічну систему у вигляді бази знань (експертні системи).

Більшість створених сьогодні систем навчання орієнтовані на аналіз механізму отримання знань людиною та їх відтворення в комп'ютерах чи інших технічних системах. Відповідно, дедуктивні методи передбачають проведення деякої роботи, що пов'язана з отриманням знань, якими володіє конкретна особа (експерт). Отримані знання організовуються в БЗ на основі ПЗБ. Найпоширенішими методами отримання знань в експертних системах є: отримання знань шляхом створення робочої групи; оперативне створення прототипу; застосування підходу „особлива увага аналізу знань"[7].

Індуктивні методи (або навчання за прецедентом) – базуються на виявленні закономірностей в емпіричних даних (так зване машинне навчання).

Індуктивне або машинне навчання являють собою процес, у результаті якого машина (комп'ютер чи технічна система) здатна відтворювати поведінку, яка в неї була явно закладена [8, 9]. Тобто загальна схема підсистеми отримання знань та навчання [10] вузлової ІСУ з використанням методів машинного навчання.

Головною відмінністю схеми машинного навчання від експертних систем є те, що людина-експерт приймає участь у формуванні БЗ лише на етапі проектування ІСУ.

Експерт задає навчальну вибірку, на основі якої вузлова ІСУ буде шукати закономірності в службовій інформації, що надходить від підсистеми контролю та збору інформації про стан МР. У процесі повторення однотипних експериментів, з використанням методів навчання, відбувається модифікація закладених експертом правил, у результаті чого на кожному наступному етапі вузлова ІСУ демонструватиме кращі результати з прийняття управлінських рішень за кожною з функціональних підсистем, ніж на попередньому етапі.

Поняття машинне навчання утворилося в результаті розділення науки про нейронні мережі на методи навчання мереж і види топологій архітектури мереж, а також увібрало в себе методи математичної статистики [1]. У зв'язку з цим, представлена класифікація методів індуктивного, тобто машинного навчання, які тісно переплітатися з методами навчання нейронних мереж.

За формою отримання знань, що залежить від здатності ІСУ формалізувати знання, методи отримання знань поділяються на такі, що отримують: знання без логічних висновків; знання „ззовні"; знання з прикладів; знання на метарівні.

За способом навчання отримання знань поділяються на наступні методи: навчання з учителем; навчання з підкріпленням; навчання без учителя; активне навчання.

Таким чином, отримання знань в ІСУ реалізується в процесі отримання деякої службової інформації про предметну область, її систематизації та подання в певній формі. Причому, форма подання знань для їх використання в ІСУ визначається особливостями об'єкта управління та інтелектуальними можливостями, які закладаються в ІСУ щодо формалізації службової інформації до рівня знань про предметну область.

Від цього залежить використання того чи іншого методу подання знань при проектуванні ІСУ.

ІІ. Методи подання знань ІСУ.

Являються сукупністю методів, способів, форм, відображення та формалізації знань. Методи подання знань бувають наступні: семантичні мережі; логіка предикатів; фреймові системи; продукційні правила; нейронні мережі; нечітка логіка.

Властивості наведених вище методів подання знань, з урахуванням їх відношення до класифікації методів обробки знань про ситуацію в МР (рис. 3), узагальнено в табл. 1. Отже, через особливості функціонування МР (часті зміни топології МР, непередбачуваний характер їх функціонування, тощо) подолати нечіткість знань про стан вузлів МР та радіомережу в цілому дуже складно як на етапі проектування, так і на етапі оперативного управління МР. З одного боку, на етапі проектування ІСУ вона міститиме базовий набір знань, отриманих від спеціалістів у даній предметній області, які мають вербальний характер та є наближеними. З іншого боку, в процесі оперативного управління МР, ІСУ повинна автоматично підтримувати базу знань про ситуацію в МР (самонавчатися), що в режимі реального часу є дуже складним завданням.

За таких умов, як видно з табл. 1, найбільш доцільним і перспективним підходом до побудови ІСУ є комплексне використання апарата нечіткої логіки, продукційних правил та нейронних мереж. Це пояснюється тим, що зазначений математичний апарат дає змогу оперувати лексичними категоріями оцінок, сприйняттям та способами мислення експерта, що особливо важливо на етапі проектування ІСУ, адже значно полегшить початкове навчання ІСУ, так як апарат нечіткої логіки, який оперує лінгвістичними змінними, дозволяє найбільш точно реалізувати машинну інтерпретацію знань експертів. Разом з тим, застосування методів нейронних мереж для побудови правил нечітких продукцій забезпечить здатність ІСУ навчатися на власному досвіді. Виходячи з вищевказаного доцільно розглянути біль детально деякі методи подання знань [1].

Таблиця 1

Властивості методів подання знань

Властивість / Метод	**Форма отримання знань**	**Спосіб навчання**	**Обсяги інформації БЗ**	**Спосіб реалізації**	**Відносна швидкодія**
Семантичні мережі	Інформація без логічних висновків. Знання „ззовні”.	З учителем. З підкріпленням	Малі, середні.	Програмний, апаратний.	Низька.
Логіка предикатів	Інформація без логічних висновків. Знання „ззовні”.	З учителем. З підкріпленням	Середні, високі.	Програмний.	Середня.
Фреймові системи	Інформація без логічних висновків. Знання „ззовні”.	З учителем. З підкріпленням	Малі.	Програмний.	Середня.
Продукційні правила	Інформація без логічних висновків. Знання „ззовні”.	З учителем. З підкріпленням	Малі, середні.	Програмний.	Середня.
Нечітка логіка	Знання „ззовні”. Знання з прикладів.	З учителем. З підкріпленням Активне Навчання.	Великі.	Програмний, апаратний.	Висока (програмна реалізація), Низька (апаратна реалізація).
Нейронні мережі	Знання „ззовні”. Знання з прикладів.	З учителем Без учителя Активне навчання	Великі.	Апаратний	Висока.

Продукційні правила. Це правила виду ЯКЩО „Умова” – ТО „Дія”, які описують знання у вигляді взаємозв’язків типу: „причина” – „наслідок”, „явище” – „реакція”, „ознака” – „факт” і т.п., в залежності від сутності знань, які подаються. Продукційне подання знань з людської точки зору є прямим описом логічних висновків при вирішенні конкретних завдань. Сукупність знань про конкретну предметну область в цьому випадку подається у

вигляді відповідного набору продукційних правил, з яких формується БЗ. При побудові продукційних правил допустиме використання логічних операторів І, АБО.

Перевагами продукційних правил є простота аналізу, доповнення, модифікації та анулювання певних продукційних правил. Крім цього, подання знань в такому синтаксично однотипному вигляді суттєво полегшує технічну реалізацію системи використання знань.

Недоліками продукційних правил можна вважати відсутність явних зв'язків між правилами і цілями, досягнення яких прагне ІСУ. Тобто, для активізації одного з продукційних правил необхідна перевірка всієї продукційної БЗ, що при великих обсягах інформації призводить до істотних витрат часових і технічних ресурсів ІСУ.

Нейронні мережі, вважаються одним з найбільш перспективних напрямків у галузі штучного інтелекту.

В основі функціонування нейронних мереж лежать принципи моделювання роботи людського мозку.

Особливостями нейронних мереж вважається: простий функціональний елемент – нейрон; значна кількість нейронів приймає участь в процесі обробки інформації; один нейрон пов'язаний з великою кількістю інших нейронів (глобальні зв'язки); ваги зв'язків між нейронами змінюються; масована паралельність обробки інформації.

Найважливішою властивістю нейронних мереж є їх здатність навчатися і в результаті навчання підвищувати свою продуктивність. Підвищення продуктивності відбувається з часом, відповідно до певних правил. Навчання на основі нейронної мережі відбувається за допомогою інтерактивного процесу коригування синаптичних ваг і порогів. В ідеальному випадку нейронна мережа отримує знання на кожній ітерації процесу навчання.

В свою чергу, нейронна мережа являє собою універсальну модель-апроксиматор у вигляді графа, головною рисою якої є використання зв'язків різної ваги між нейронами як засобу для запам'ятовування інформації.

Обробка інформації нейронними мережами ведеться одночасно великою кількістю елементів, завдяки чому вони стійкі до несправностей та здатні до швидких обчислень. Задати нейронну мережу, здатну вирішити конкретну задачу, це значить визначити модель нейрона, топологію та ваги зв'язків між нейронами. Слід зазначити, що нейронні мережі, призначені для вирішення різних завдань, менше всього відрізняються одна від одної моделями нейрона. Найважливішою властивістю нейронних мереж є їх здатність навчатися і в результаті навчання підвищувати свою продуктивність. Підвищення продуктивності відбувається з часом, відповідно до певних правил. Навчання на основі нейронної мережі відбувається за допомогою інтерактивного процесу коригування синаптичних ваг і порогів. В ідеальному випадку нейронна мережа отримує знання на кожній ітерації процесу навчання.

Тому, будуючи модель шляхом навчання, за рахунок модифікації ваг міжелементних зв'язків, нейронна мережа здатна підвищувати свою адекватність.

Перевагами нейронних мереж є малі об'єми пам'яті, необхідні для зберігання нейронів, висока адаптивність, а також здатність до опрацювання нечіткої та неповної інформації, що дозволяє застосовувати нейронні мережі практично в будь-якій предметній області, в тому числі, при вирішенні задач прогнозування складних процесів.

Недоліками нейронних мереж є відсутність наочності подання знань, адже образи, які запам'ятала мережа під час навчання, закодовані у вигляді станів усіх нейронів мережі, а процес прийняття рішень у мережі не може бути представлений у вигляді наглядних конструкцій ЯКЩО – ТО.

Крім того, методи навчання нейронних мереж залежать від їх структури, що потребує розробки нового методу в залежності від конкретного випадку застосування нейронної мережі.

Нечітка логіка. Серед усіх відомих засобів моделювання, теорія лінгвістичної змінної, що базується на нечітких множинах [11], дозволяє найкращим чином здійснювати строгу математичну формалізацію логіко-лінгвістичної інформації, яка застосовується при описі складних нелінійних об'єктів. Як правило, моделювання таких об'єктів зводиться до

побудови нечітких баз знань, які втілюють в собі експертні знання про об'єкт у вигляді лінгвістичних висловлювань ЯКЩО-ТО.

Основним формалізмом теорії нечітких множин, за допомогою якого експертні знання ЯКЩО-ТО перетворюються на суворі математичні моделі, є поняття функції належності [12], яка характеризує суб'єктивну міру впевненості експерта в тому, що деяка величина належить певному нечіткому поняттю (терму), яким характеризується та чи інша вхідна (вихідна) змінна.

З метою логічного зв'язку функцій належності вхідних і вихідних змінних в рамках теорії нечітких множин сформульовані методи нечіткого логічного висновку.

Перевагами нечіткої логіки вважається наочність подання знань шляхом використання лінгвістичних висловлювань ЯКЩО-ТО, нечітка логіка надає можливість оперувати вхідними даними, заданими нечітко: наприклад, що безупинно змінюються в часі значення (динамічні задачі), проводити нечітку формалізацію критеріїв оцінки і порівняння: оперування критеріями „більшість", „можливе", „переважно" і т.д.; можливість проведення швидкого моделювання складних динамічних систем і їхнього порівняльного аналізу із заданим ступенем точності.

Недоліки нечіткої логіки полягають в тому, що, оскільки функції належності мають суб'єктивний характер, якість побудованої нечіткої моделі повністю залежить від кваліфікації експерта, який сформулював правила ЯКЩО-ТО і вибрав ті чи інші форми функцій приналежності.

У зв'язку з цим, результати нечіткого логічного висновку іноді можуть помітно відрізнятися від реальних експериментальних даних, тому виникає задача налаштування параметрів нечіткої моделі за експериментальними даними за аналогією з теорією ідентифікації [1].

Отримані знання можна поділити на емпіричні (знання отримані на основі досвіду або спостереження) та теоретичні (знання отримані на основі аналізу абстрактних моделей).

У таблиці 2 наведена порівняльна характеристика, властивості, можливості, критерії , переваги та недоліки.методів навчання БЗ в СЗБ.

1. S. More, M. Matthews, A. Joshi, T. Finin. Розглянутий метод використовується в системах забезпечення безпекою для запобігання порушень безпеки зі здатністю прогнозування подій. Запропонований метод дозволяє отримувати теоретичний тип знань за наступними формами: отримання знань „ззовні" та отримання знань з прикладів. Цей метод здатний навчати базу знань з учителем та з підкріпленням.

Даний метод має семантичну інтеграцію з web-тексту і сенсорної інформації IDS / IPS.

Перевагами методу є: можливість сканування мережі, отримання та подання знань, можливість виявлення атак, формування БЗ з окремих вузлів.

До недоліків методу можна віднести: неможливість використання у мережі з динамічною топологією, відсутність надання управлінського рішення, обмежені можливості обробки інформації в умовах нечіткої мережевої активності [13].

2. M. S. Ahmad. Розглянутий метод використовується в СЗБ. БЗ навчаються на основі мобільних та гнучких агентів.

Запропонований метод дозволяє отримувати теоретичний тип знань за наступними формами: отримання знань „ззовні" та отримання знань з прикладів.

Цей метод здатний навчати базу знань з учителем та з підкріпленням. Даний метод дозволяє гнучко взаємодіяти агентам протягом малого проміжку часу, щоб виявити атаку в реальному часі.

Перевагами даного методу є навчання на основі мобільних та гнучких агентів, велика швидкодія, самонавчання БЗ.

До недоліків даного методу відноситься неможливість використання у мережі з динамічною топологією та залежність від центральної системи управління [14].

Таблиця 2

Практичні методи навчання баз знань

Властивість / Метод	Форма отримання знань	Тип отриманих знань	Спосіб навчання	Обсяги інформації в БЗ	Практична складова	Критерії оцінки
S. More, M. Matthews, A. Joshi, T Finin	Знання „ззовні”; Знання з прикладів.	Теоретичні	З учителем; З підкріпленням.	Малі, середні.	Інтелектуальна IDPS.	Точність–52.3 Компактність–68.2
M. S. Ahmad	Знання „ззовні”; Знання з прикладів.	Теоретичні	З учителем; З підкріпленням.	Великий.	Інтелектуальна IDS.	Точність–57.4 Компактність–69.2
S. Shtavbo	Інформація без логічних висновків; Знання „ззовні”.	Емпіричні	З учителем; З підкріпленням; Активне навчання.	Малі.	Інтелектуальна систем оцінки ризиків.	Точність–57.7 Компактність–69.4
H.I-M. Sayedahmed O.S.Fargalla	Знання „ззовні”; Знання з прикладів.	Теоретичні	Без учителя; З підкріпленням.	Середні.	Інтелектуальна система аудиту та IDS.	Точність–58.4 Компактність–69.7
O.Oriola, A.B.Adeyemo O.Osunade	Інформація без логічних висновків; Знання з прикладів.	Теоретичні Емпіричні	З учителем; З підкріпленням; Активне навчання.	Великі.	Система прогнозування попередження та IPS.	Точність–62.2 Компактність–71.6
H. Ishibuchi, T. Nakashima T. Murata	Знання „ззовні”; Знання з прикладів.	Теоретичні Емпіричні	З учителем; Активне Навчання.	Великі.	Інтелектуальна система ідентифікації та IDS.	Точність–63.5 Компактність–70.8

3. S. Shtavbo. Розглянутий метод баз знань побудований на основі мережі Мамдані використовується в системах забезпечення безпекою для оцінки ризиків запобігання. Запропонований метод дозволяє отримувати емпіричний тип знань за наступними формами: отримання знань „ззовні” та отримання знань з інформація без логічних висновків. Цей метод здатний навчати базу знань з учителем, з підкріпленням та на основі активного навчання.

Перевагами даного методу є: компактність БЗ, здатність формування нечітких правил, самонавчання. До недоліків даного методу відноситься неможливість використання у мережі з динамічною топологією, відсутність надання управлінського рішення, відсутня знатність формування БЗ з окремих вузлів [15].

4. H. I-M. Sayedahmed, O. S. Fargalla, N. A. Elfeshawy. Розглянутий метод використовується в системах забезпечення безпекою для аудиту та виявлення порушень безпеки, побудований на основі нейронної мережі. Запропонований метод дозволяє отримувати теоретичний тип знань за наступними формами: отримання знань „ззовні” та отримання знань з прикладів. Цей метод здатний навчати базу знань з учителем та з підкріпленням.

Перевагами методу є: адаптивність до роботи в мережі з динамічною топологією, здатність працювати при різних станах та параметрах нейронної мережі зі зворотнім поширенням тобто самонавчання. Недоліками цього методу є: не адаптивність до роботи з іншими підсистемами забезпечення безпеки, мала продуктивність наповнення БЗ, залежність від центральної системи управління [16].

5. O. Oriola, A. B. Adeyemo, O. Osunade. Розглянутий метод використовується в системах забезпечення безпекою для попередження та запобігання вторгнень в мережу, побудовану на основі продукційних правил та нечіткої логіки. Запропонований метод дозволяє отримувати теоретичний та емпіричний тип знань за наступними формами: отримання знань з інформації без логічних та отримання знань з прикладів. Цей метод здатний навчати базу знань з учителем, з підкріпленням та на основі активного навчання.

Перевагами методу є: формування знань з неповної та нечіткої інформації, адаптивність до пасивних підсистем забезпечення безпеки, формування БЗ з окремих вузлів та здатність прогнозування. Недоліками даного методу є: не пристосування до роботи в мережах з динамічною топологією, контроль загрози проводиться у внутрішній зоні мережі, відсутність надання приймання управлінського рішення відносно можливих подій в МР або впливів на мережу [17].

6. H. Ishibuchi, T. Nakashima, T. Murata. Розглянутий метод використовується в системах забезпечення безпекою для ідентифікації та виявлення вторгнень мережі, побудований на нечіткій логіці з використанням нечіткого класифікатора та гібридного алгоритму. Запропонований метод дозволяє отримувати теоретичний та емпіричний тип знань за наступними формами: отримання знань „ззовні" та отримання знань з прикладів. Цей метод здатний навчати базу знань з учителем та на основі активного навчання.

Переваги методу є: формування знань з неповної та нечіткої інформації, використання в радіомережі, формування БЗ з окремих вузлів. Недоліками даного методу є: непристосованість до роботи в мережах з динамічною топологією, відсутність надання управлінського рішення відносно можливих подій у МР або впливів на мережу [19].

Аналіз функціонування методів навчання БЗ оцінюються з наступних критеріїв:

Критерій точності - з точністю роботи пов'язані такі характеристики, як: правильність виконуваних висновків, адекватність бази знань проблемної області, обґрунтованість застосованих методів вирішення проблеми.

Критерій компактності - враховує кількість вхідних змінних, кількість правил у базі знань, кількість коротких правил у базі знань, сумарну довжину антецедентів правил бази знань, потужності терм-множин вхідних змінних, рівень наповненості бази знань правил, кількість параметрів бази знань тощо.

Таким чином найбільшою мірою представленим вимогам та за критеріями відповідають методи [17, 18], які реалізовані для використання в інтелектуальних системах забезпечення безпеки, що має схильність до масштабування. Дані методи побудовані зі здатністю подання знань, а також можливістю прийняття рішень в сенсорних мережах нечіткої логіки та прогнозуванні. Однак, запропоновані методи не реалізують можливість самонавчання щодо забезпечення безпеки при поданні новизни на вузлах та мережі з динамічною топологією, та непристосовані до застосування при непередбачуваній, неповній, нечіткій мережевій активності.

ВИСНОВОК

Проведений аналіз показав, що існуючі методи, в основному, здатні вирішувати завдання з подання та отримання знань в інтелектуальних системах забезпечення безпеки у проводових мережах або у стаціонарних радіомережах, що в свою чергу, не задовольняє вказаним вище вимогам, щодо застосування даних методів у мобільній радіомережі тактичної ланки управління військами. Тому при розробці баз знань інтелектуальних систем забезпечення безпеки доцільно застосувати комплексне поєднання нечіткої логіки, продукційних правил та нейронних мереж.

У ході подальших досліджень будуть розроблені методи навчання баз знань в системах забезпечення безпеки в мобільних радіомережах із застосуванням нечіткої логіки, продукційних правил та нейронних мережах.

ЛІТЕРАТУРА

1. Сова О.Я., Методи обробки знань про ситуацію в мобільних радіомережах класу MANET для побудови вузлових інтелектуальних систем управління / Сова О.Я., Романюк В.А., Міночкін Д.А., Романюк А.В. // Збірник наукових праць ВІТІ ДУТ. – 2014. – № 1. – С. 97 – 110.

2. Романюк В.А. Архітектура системи оперативного управління тактичними радіомережами / Романюк В.А. // Збірник наукових праць ВІТІ НТУУ „КПІ”. – 2009. – № 3. – С. 70 – 76.

3. Zhuk P., Intellectual Mobile Ad Hoc Networks / Zhuk P., Romanyuk V., Sova O., Bunin S. // In Proc. of International Conference Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET 2012), Lviv, 2012. – P. 238.

4. Романюк В.А. Цільові функції оперативного управління тактичними радіомережами / Романюк В.А. // Збірник наукових праць ВІТІ– 2012. –№ 1.– С. 109 – 117.

5. Гаврилова Т.А. Базы знаний интеллектуальных систем: Учебник для вузов / Т.А. Гаврилова, В.Ф. Хорошевский. – СПб.: Питер, 2000. – 384 с.

6. Рубанов В.Г. Интеллектуальные системы автоматического управления. Нечеткое управление в технических системах: учебное пособие / В.Г. Рубанов, А.Г. Филатов. – Белгород: Изд-во БГТУ им. В. Г. Шухова, 2010. – 170 с.

7. Мітюшкін Ю.І. Soft Computing: ідентифікація закономірностей нечіткими базами знань. Монографія / Мітюшкін Ю.І., Мокін Б.І., Ротштейн О.П. –Вінниця, 2002. – 145 с.

8. Samuel A.L. Some Studies in Machine Learning Using the Game of Checkers /Samuel A.L. // IBM Journal. – July 1959. P. 210 – 229.

9. Wang L. Machine Learning for Human Motion Analysis / Wang L., Cheng L., Zhao G. – IGI Global, 2009. – 318 p.

10. Романюк В.А. Концепція ієрархічної побудови інтелектуальних систем управління мобільними радіомережами військового призначення / Романюк В.А., Сова О.Я., Жук П.В. // Збірник наукових праць ВІТІ НТУУ „КПІ”. – 2010. – № 2. – С. 121 – 130.

11. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику / Штовба С.Д. – Винница: Континент-Прим. – 2003. – 198 с.

12. Макаров И.М. Искусственный интеллект и интеллектуальные системы управления / Макаров И.М., В.М. Лохин, С.В. Манько, М.П. Романов; Отделение информ. технологий и вычислит. систем РАН. – М.: Наука, 2006. – 333 с.

13. S. More A Knowledge-Based Approach To Intrusion Detection Modeling /S. More, M. Matthews, T. Finin// Proceedings of the IEEE Workshop on Semantic Computing and Security 2012 – P. 75 – 81.

14. Patel A. An intrusion detection and prevention system in cloud computing: A systematic review /A.Patel, M.Taghavi, K.Bakhtiyari, J.Junior//Journal of Network and Computer Applications 36 (2013) – P. 25 – 41.

15. Shtavbo S. Learning compact fuzzy knowledge bases for systems security type Mamdani / S. Shtavbo // luwer Academic Publisher, 2014. – 283p.

16. Hassan I.M. Sayedahmed Neural Network Algorithms Performance Measure for Intrusion Detection/ Hassan I.M. Sayedahmed, Osama S. Fargalla, Nawal A. Elfeshawy// Proceedings of the 5th WSEAS International Conference on MBE – 2009. – P. 61 – 67.

17. Oriola O. Network Threat Characterization in Multiple Intrusion Perspectives using Data Mining Technique / O.Oriola, A. B. A.and O. Osunade / (IJNSA), Vol.4, No.6. – 2012.

18. Ishibuchi H. Three-objective genetics-based machine learning for linguistic rule extraction / H. Ishibuchi, T. Nakashima, T. Murata // Inform. Sci. – 2001. – Vol. 136, No. 1. – P. 109 – 133.