УДК 621.391

С.В. Сальник, В.В. Сальник, Е.М. Бовда

Військовий інститут телекомунікацій та інформатизації, Київ

МЕТОДИКА АУДИТУ ВТОРГНЕНЬ В МОБІЛЬНІ РАДІОМЕРЕЖІ КЛАСУ MANET

В статті представлена методика аудиту вторгнень в мобільні радіомережі класу MANET. Розробка методики базувалася на алгоритмі дій, який включає в себе етапи та кроки проведення аналізу, моніторингу даних та тестування мобільної радіомережі. Було запропоновано підхід проведення аудиту, який ґрунтується на використанні нейронної мережі з можливістю проведення самонавчання, роботі при нечіткій мережевій активності, в умовах режиму реального часу та параметрів, якими характеризується мобільна радіомережа. Розроблена методика проведення аудиту вторгнень в мобільну радіомережу дозволяє підвищити ефективність надання управлінських рішень, спростити процес проведення аналізу, моніторингу та тестування мережі, а також слугувати основою для розробки програмного продукту для проведення аудиту рівня безпеки мобільної радіомережі. Визначено подальший напрямок роботи, щодо побудови нечіткої бази знань, яка покращить проведення аудиту мережі та підвищить рівень безпеки мобільної радіомережі.

Ключові слова: *мобільні радіомережі, MANET, аудит вторгнень.*

Вступ

Актуальність дослідження. Останнє десятиліття спостерігається динамічний розвиток та поширення мобільних радіомереж (МР) класу MANET (*Mobile Ad-Hoc Networks*) [1]. У зв`язку з цим поширенням спостерігається зацікавленість у здійсненні деструктивного впливу на процес функціонування МР з метою порушення цілісності, доступності, конфіденційність інформації, яка передається в МР або для впливу на інформаційну, програмна або апаратну частину мережі.

З метою недопущення даного впливу на МР, забезпечення безпеки мережі покладається на систему виявлення вторгнень (СВВ), функціонування якої здійснюється на основі методів виявлення вторгнень (МВВ) [2].

На СВВ покладається завдання щодо проведення аналізу, класифікації та кластеризації великої кількості різнорідних параметрів трафіка МР. Враховуючі віддалене знаходження та керування компонентами МР, до СВВ висуваються наступні вимоги: енергоефективність, простота побудови, проведення складних та різнорідних розрахунків та інше. Тому з метою забезпечення безпеки МР, елементи СВВ повинні розміщуватись на вузлах МР. Вузлова СВВ повинна містити у своєму складі методи проведення аудиту даних до якого належить збір аналітичних, моніторингових даних та оцінка факторів, які визначають рівень захищеності мережі. Ці фактори відображаються у стандартах та вимогах висуваємих до рівня захищеності мережі [3].

З метою забезпечення безпеки під час вторгнення в МР та враховуючи особливості функціонування сучасних МР, необхідно проводити аналіз, тестування та моніторинг мережі з урахуванням множини вразливостей мережі, типів вторгнень та ризиків здійснення вторгнень в МР, що в цілому відповідатиме аудиту мережі.

Аудит МР представляє собою перевірку мережі, системи безпеки, систем які забезпечують взаємодію з іншими компонентами МР на предмет не відповідності поточної інформаційної ситуації стандартам інформаційної безпеки [4]. Таким чином аудит являє собою перевірку стану МР та порівняння цього стану з еталоном стану рівня безпеки мережі. До робіт, які розглядають основні етапи проведення аудиту та питання забезпечення безпеки МР відносяться [5, 6, 17].

Тому з урахуванням стрімкого розвитку мобільних комунікацій, які обмежують можливість швидкої адаптації існуючих СВВ до нових загроз, та взаємодію елементів МР з елементами стаціонарної інфраструктури, які значно розширюють варіанти впливу на мережу та СВВ [3,7], робить актуальним питання проведення аудиту безпеки мережі з метою забезпечення безпеки МР.

Метою роботи є розробка методики аудиту вторгнень в МР класу MANET, яка дозволить надати управлінські рішення, щодо вторгнення в мережу та покращить ефективність роботи СВВ.

Об'єктом розгляду даної статті є процес забезпечення безпеки інформації, яка передається в МР.

Предметом дослідження **є** методика аудиту вторгнень в МР класу MANET.

Результати досліджень

Аналіз предметної області. У зв`язку з тим, що СВВ потрібно виявляти вторгнення, у МР та у систему управління нею [3, 8], то СВВ повинна відслідковувати весь трафік, що циркулює в МР. Для цього СВВ забезпечує своє функціонування на всіх рівнях моделі OSI, здійснюючи при цьому моніторинг з`єднань, аналіз трафіка та інше.

На сьогоднішній день аудит безпеки стає все більш розповсюдженим при організації безпеки проводових мереж. Однак використання аудиту в безпроводовому середовищі обмежено всього декількома публікаціями та рішеннями.

Аудит проводить обрахування рівня захищеності МР ґрунтуючись на множину вразливостей мережі та способів реалізації загроз при проведенні вторгнень за допомогою різнонаправлених атак. Сутність аудиту полягає у перевірці та тестуванні параметрів мережі щодо її стану за допомогою відповідних підходів [9].

Основними вимогами до функціональних можливостей розробляємої методики на підставі аналізу предметної області повинні бути наступні: проведення самонавчання бази знань; збір даних стану мережі та тестування мережі; моніторинг стану роботи засобів безпеки мережі; формування багатокритеріального опису стану захищеності мережі, проведення класифікації та кластеризації параметрів мережі; надання управлінських рішень, щодо покращення рівня безпеки мережі.

Виходячи з вказаного основними критеріями оцінки проведення аудита мережі буде: рівень повноти бази знань, рівень збору інформації, рівень розподілу вхідних даних на класи та типи, рівень надання управлінського рішення.

Позначення вихідних даних: Вхідними даними є інформаційна, програмна, апаратна складова МР та СВВ, що складається із множини контрольних точок, що підлягають перевірці та множини зв`язків між контрольними точками та джерелами інформації.

Вихідними даними є класифікована, аналізована та перевірена на відповідність стандартам безпеки множина даних, яка характеризує поточний стан безпеки МР.

Обмеження та допущення: Для визначення можливих обмежень та допущень потрібно врахувати необхідність прийняття управлінського рішення на підставі аналізу вторгнень, які здійснюються на МР практично на всіх рівнях мережевої моделі OSI. В свою чергу МР складається із програмної, апаратної, інформаційної складових, які можуть бути оцінені за різними параметрами. З цього виходить що, кількість типів та варіантів впливів на мережу може бути необмеженою.

А навчальна множина бази знань, яка застосовується на різних етапах проведення аудиту є обмеженою. Тобто розрахунок обмежено наявністю кожного нового аномального явища, яке буде відбуватися в мережі. Дана методика допускає збір даних з контрольних точок мережі та проведення тестування СВВ мережі. Тестування допускає збір даних у СВВ, яка працює з чіткими даними або при нечіткій мережевій активності. Надання управлінських рішень відбувається на основі співставлення отриманих даних та обмежено повнотою бази знань.

На підставі викладеного необхідно розробити методику аудиту вторгнень в МР класу MANET.

Проведення аудиту можливо поділити на етапи, які визначають порядок дій та функцій, щодо забезпечення безпеки МР.

1 етап – планування та підготовка до аудиту

Підготовка та планування аудиту забезпечує системність під час аудиту мережі, визначає пріоритетність перевірки складових частин мережі, встановлює політику безпеки та враховує можливу нечітку мережеву активність мережі. Виконання цього етапу також передбачає визначення: інформаційної архітектури, технологічного напрямку, організаційних аспектів та підрахування ризиків.

До цього етапу входить: визначення мети планування, визначення об`єктів аудиту, визначення мети збору даних, визначення методів збору даних, визначення допустимих меж проведення аудиту, визначення стандартів проведення аудиту, визначаються контрольні точки для перевірки інформаційних, програмних та апаратних складових мережі, визначення вагових пріоритетів отриманих даних та визначення меж отримання нечітких параметрів [9].

Основною задачею даного етапу є вибір типу, структури та алгоритму роботи обчислюваної мережі. Як вказано у [2, 3], з метою проведення складних обчислень, кластеризації та класифікації різнорідних даних, які характеризуються нечіткою мережевою активністю, доцільно використовувати нечіткі нейронні мережі. Аналіз вказує, що найбільш пристосованими нейронними мережами для виконання вказаної мети є: нечіткий багатошаровий перцептрон, мережа Кохонена, мережа Хопфілда, Елмана та інші.

Варіантом структури нейронної мережі, для аудиту рівня захищеності може бути прийнята мережа, що складається з наступних шарів:

1 шар – Терм вхідних змінних. У даному шарі відбувається перетворення вхідних даних до нечіткого вигляду. Тобто вихідним значенням шару буде ступінь належності значень вхідної змінної її відповідному нечіткому терму;

2 шар – Антецеденти нечітких правил. У даному шарі кожен нейрон відповідає одному нечіткому правилу. Вихідним значенням шару є ступінь відповідності правилу;

3 шар – Завершення правил. В даному шарі нейрони обраховують внесок нечіткого правила в вихід мережі;

4 шар – Агрегування результатів. Нейрон цього шару сумує та інтерпретую внески всіх правил.

Основною метою нейронної мережі є перетворення набору множини вхідних даних до відповідної

множини вихідних даних. Тому, ефективність рішення даної задачі залежить від архітектури нейромережі та її навчання.

Вибір архітектури нейромережі відповідатиме такій мережі, яка буде виконувати свою функцію з мінімальною похибкою:

$$E(\omega) = \frac{1}{2}\sum_{j=1}^{p}\left(y_j - d_j\right), \qquad (1)$$

де y_j – значення j-го виходу нейромережі;

d_j – цільове значення j-го виходу;

p – кількість нейронів у вихідному шарі.

Для перевірки результатів навчання використовуються тестові данні. З метою оцінки якості побудованою мережі використовується середня похибка апроксимації $\overline{A}$, яка визначається як середнє значення відносних відхилень розрахункових значень F_i від фактичних F.

$$\overline{A} = \frac{1}{n}\sum\left|\frac{F_i - F}{F_i}\right| \times 100\%. \qquad (2)$$

Наступним кроком є побудова бази знань, яка забезпечить проведення аудиту на всіх її етапах.

База знань представляє собою особливого роду базу правил, яка містить структуровану, подану в певній формі інформацію про стан компонентів та складових частин МР в цілому, котра використовується для прийняття управлінських рішень на різних рівнях моделі OSI.

Основними особливостями баз знань є: здатність формування висновків у автоматичному режимі. [10,11], здатність знаходити протиріччя, які можуть виникнути в ній самій (інтроспекція), здатність адаптуватися до нових умов функціонування, проведення самонавчання, можливість рішення задач класифікації та кластеризації, можливість проведення адаптації мережі для роботи при нечіткій мережевій активності, наявність в мережі обернених зв'язків, можливість проведення навчання в режимі реального часу.

Виходячи із вказаних особливостей та враховуючі завдання щодо проведення аудиту вторгнень МР доцільно застосовувати базу знань на основі методу навчання Хебба, яка складається з таких рівнів [12, 21]:

1 рівень – ініціалізація, на якому ваговим коефіцієнтам присвоюються невеликі випадкові значення.

2 рівень – на входи мережі подається вхідний образ, і сигнали збудження розповсюджуються по всім шарам відповідно принципів класичних прямо потокових мереж [13], тобто для кожного нейрону розраховується зважена сума його входів, до якої застосовується активаційна (передаточна) функція нейрону, в результаті чого отримуємо його вихідне значення.

3 рівень – на основі отриманих вихідних значень нейронів здійснюється зміна вагових коефіцієнтів.

4 рівень – цикл повертається до другого етапу до тих пір поки значення мережі не стабілізуються з заданою послідовністю.

2 етап – збір необхідних даних

До цього етапу входить:

Визначення умов забезпечення безпеки мережі, збір даних з використанням методу аналізу та моніторингу, оцінка аналізу та моніторингу стану мережі та побудова стану показників, оцінка системи забезпечення безпеки, отримання незалежної оцінки.

На даному етапі відбувається аналіз роботи джерел на підставі перевірки контрольних точок. Аналіз відбувається з використанням методу перевірки, який застосовується відповідного до типу контрольної точки [14].

Збір даних стану мережі, ґрунтується на аналізу множини вразливостей, множини варіантів проведення вторгнень, часу, частоти вторгнень та інше. В основі проведення цього кроку знаходиться модель вторгнень в МР та видів застосовуваних атак на рівнях мережевої моделі OSI. На основі вказаного будуть отримані аналітичні вирази для оцінки ймовірності порушення безпеки МР на рівнях мережевої моделі OSI. Тобто значення ймовірності вторгнення на окремому рівні моделі OSI в загальному вигляді матиме вигляд:

$$R = P_Z \cdot P_V \cdot \varpi, \qquad (3)$$

де P_Z – ймовірність реалізації типу вторгнення на окремому рівні моделі OSI;

P_V – ймовірність використання вразливостей на окремому рівні моделі OSI;

ϖ – коефіцієнт вторгнення на окремому рівні моделі OSI.

3 етап – тестування

До цього етапу входить:

визначення мети та порядку проведення тестування,

перевірка умов встановлення та застосування обладнання,

перевірка системи захисту,

моделювання проведення вторгнення,

розрахунок інформаційних ризиків [15].

Тестування МР ґрунтується на проведенні перевірки: системи захисту МР, системи реагування на вторгнення, відповідності варіантів реагування рівню визначення довіри до мережі, відповідності варіантів реагування адекватності прийнятих рішень (дотримання стандартів).

До цього етапу відносяться такі кроки:

побудова перевіряючої бази знань,

моделювання проведення вторгнень в мережу;

розрахунок вразливостей, загроз та ризиків.

Оцінка показників рівня захищеності відбувається за шкалою від 0 до 1, де:

(0,9; 1) – високий рівень захищеності;

(0,7; 0,9) – рівень захищеності вище середнього;

(0,3; 0,7) – середній рівень захищеності,

(0,1; 0,3) – рівень захищеності нище середнього;

(0; 0,1) – низький рівень захищеності.

Виходячи із вказаного:

ймовірність здійснення j_Z типів вторгнень на множину об'єктів мережі l буде обчислюватись:

$$P(j_Z, l) = \prod_{i=1}^{l} P_i^{j_Z}; \quad (4)$$

ймовірність здійснення вдалого вторгнення на N вузол мережі шляхом застосування j_Z типів вторгнень мати вигляд:

$$P_r = \max_j P_i^j, \; j = 1...j_Z, \quad (5)$$

Враховуючі множину варіантів проведення вторгнення у мережу, для представлення повної моделі вторгнень доцільно врахувати наявність СВВ, яка забезпечує безпеку МР. Тому, якщо кожен вузол мережі має СВВ, яка направлена на виявлення вторгнень то ймовірність виявлення вторгнення буде визначатися:

$$P_B = \min_b P_i^b, \; b = 1...b_n, \quad (6)$$

4 етап – аналіз отриманих даних

До цього етапу входить: аналіз процесу обробки даних, аналіз та розрахунок різнорідних отриманих даних, моніторинг системи забезпечення безпеки, кластеризація та класифікація даних, перевірка політики безпеки, відповідність стандартам безпеки, визначення недоліків системи безпеки [16-18].

Формування різнорідного опису стану захищеності мережі, проведення класифікації та кластеризації параметрів мережі буде залежати від методів, які забезпечують роботу СВВ. З урахуванням характеристичних особливостей МР, роботі мережі при нечіткій мережевій активності та взаємодії елементів МР з елементами стаціонарної інфраструктури доцільно застосовувати МВВ, які проводять виявлення вторгнень ґрунтуючись окремо на повні (чіткі) або неповні (нечіткі) вхідні параметри даних [3].

Вихідним даними етапу є данні щодо: стану мережі, рівня мережевої активності, нечіткій активності, потенційно небезпечної активності, показників функціонування СВВ та інші значення, які характеризують типи вторгнень а також вразливості МР та СВВ.

5 етап – обробка даних та надання управлінських рішень

До цього етапу входить: аналіз чітких або нечітких даних, аналіз виконання стандартів забезпечення безпеки, формування бази знань відносно множини варіантів реагувань на порушення безпеки, оцінка дотримання стандартів, політики безпеки, ефективності мір безпеки, надання управлінських рішень відносно покращення рівня безпеки мережі, надання звітної інформації щодо стану МР [19, 20].

У разі виявленні параметрів, які характеризують порушення безпеки, нейронний шар надає значенню параметра відповідну характеристичну терму, яка свідчить про характеристики небезпеки (параметри, види впливу у МР на рівнях моделі OSI). Дана терма слугує вихідними данними для прийняття управлінських рішень щодо впливу на вторгнення відповідно до його функціонального призначення та особливості. Відповідно до бази знань, з`являється пропозиція для підсистеми реалізації рішень відносно варіантів реагування на виявлену небезпеку [3,21].

В цілому запропоновану у статті методику аудиту вторгнень у МР зазначено у вигляді схеми організації аудиту вторгнень у МР на рис. 1.

Аналізуючи етапи проведення аудиту з урахуванням методів, засобів та об`єктів проведення аудиту, вказує на те, що аналіз та моніторинг мережі має структурований, поетапний та децентралізований характер. Проведення аудиту вторгнень застосовується до об`єктів, які входять до зони відповідальності СВВ. В свою чергу аудит може мати більш складну та структуровану систему забезпечення безпеки мережі. Тобто аудит може відбуватися на кожному компоненті мережі з наданням звітної інформації від нижніх ланок мережі вищім. Дана частина мережі здатна проводити аудит мережі децентралізованим способом завдяки розташуванню СВВ на кожному компоненті мережі або розподілі функцій аудиту між СВВ нижніх та вищих ланок мережі.

Висновок

У статті представлено методика аудиту безпеки МР класу MANET на основі нейронної мережі. Запропонований підхід ґрунтується на можливості самонавчання, роботі при нечіткій мережевій активності, в умовах режиму реального часу та параметрів якими характеризується МР. Розроблена методика проведення аудиту вторгнень в МР дозволяє значно спростити процес проведення аналізу, моніторингу та тестування мережі, а також бути основою для розробки програмного продукту для проведення аудиту вторгнень в МР та тестування СВВ.

Однак для покращення роботи аудиту та з метою забезпечення безпеки МР доцільно провести побудову нечіткої бази знань на що і буде направлена подальша робота.

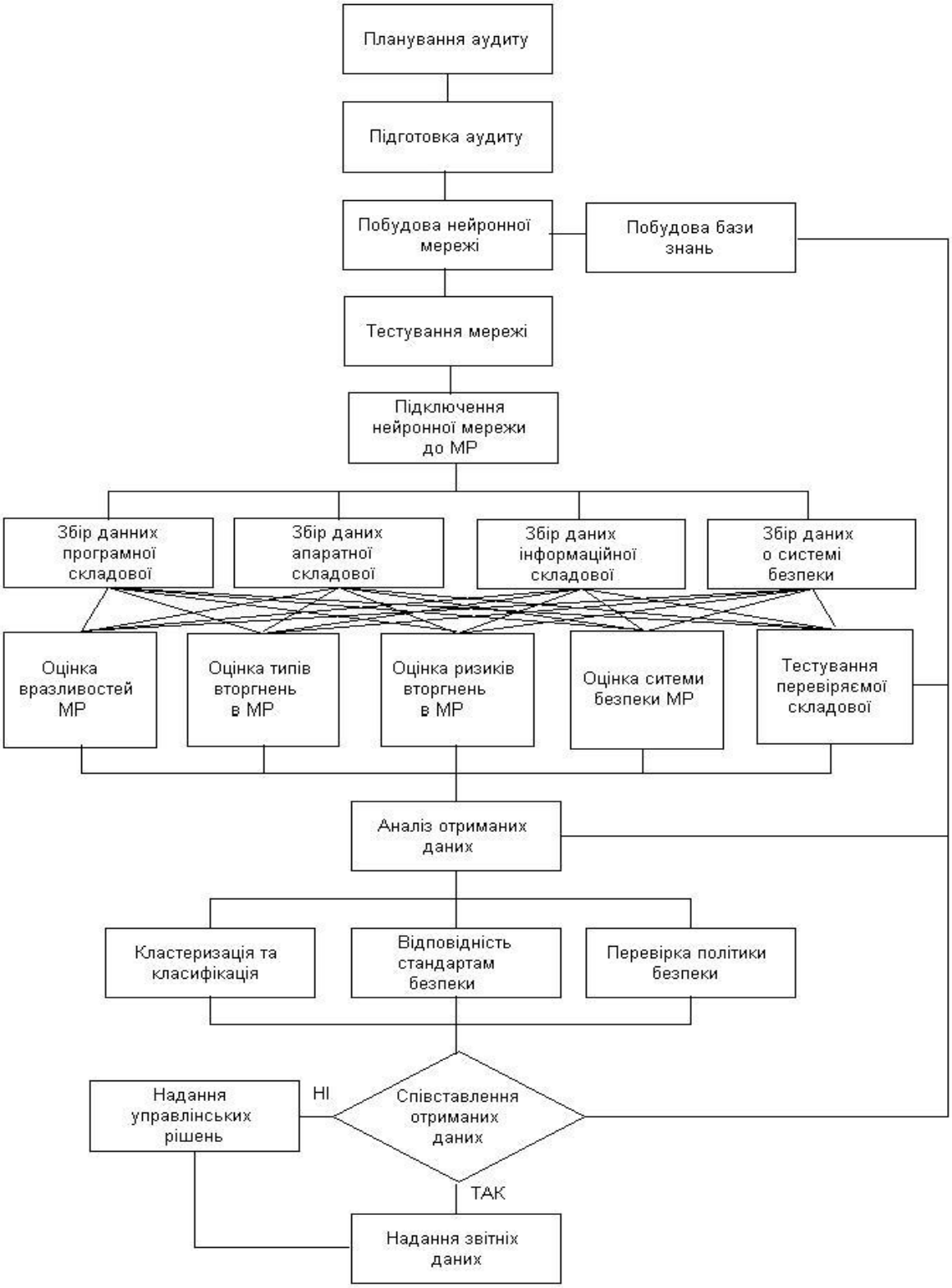

Рис. 1. Схема організації аудиту вторгнень у МР

Список літератури

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

2. Сальник С.В. Аналіз методів виявлення вторгнень у мобільні радіомережі класу MANET / С.В. Сальник, О.Я. Сова, Д.А. Міночкін // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – № 1 (22). – С. 103-112.

3. Метод виявлення вторгнень в мобільні радіомережі на основі нейронних мереж / С.В. Сальник, В.В. Сальник, О.А. Симоненко, О.Я. Сова // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – № 4 (21) – С. 82-91.

4. Голованов В.Б. Аудит информационной безопасности / В.Б. Голованов, С.Л. Зефиров, А.П. Курило // Под ред. А. П. Курило. – М.: БДЦ-Пресс; 2006. – 305 с.

5. Найханова И.В. Аудит систем менеджмента качества и информационной безопасности / И.В. Найханова // Вестник Московского государственного технического университета им. Н. Э. Баумана. Серия: Приборостроение. – 2011. – № SPEC. – С. 152-156.

6. Найханова И.В. Виды и методики аудита информационной безопасности: состояние и анализ / И.В. Найханова // Информатизация образования и науки. – 2012. – №3(15). – С. 81-94.

7. Міночкін А.І. Виявлення атак в мобільних радіомереж / А.І. Міночкін, В.А. Романюк, П.В. Шаціло // Збірник наукових праць № 1. – К.: ВІТІ НТУУ "КПІ". – 2005. – С. 102 – 111.

8. Платонов В.В. Программно - аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования // В.В. Платонов. – М.: Издательский центр «Академия», 2013. – 336 с.

9. Фомин А.А. Исследование и оптимизация алгоритмов аудита информационной безопасности организации / А.А. Фомин // Вопросы защиты информации. – М., 2009. – № 3. – С. 57–63.

10. Романюк В.А. Цільові функції оперативного управління тактичними радіомережами / Романюк В.А. // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2012. – № 1. – С. 109 – 117.

11. Бушуев С.Н. Теоретические основы создания информационно-технических систем / Бушуев С.Н., Осадчий А.С., Фролов В.М. – СПб.: ВАС, 1998. – 404 с.

12. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.: Изд. дом "Вильямс", 2006. – 1104 с.

13. Lakshmi C.J. Fusion of Neural Networks, Fuzzy Systems and Genetic Algorithms: Industrial Applications / Lakshmi C.J., Martin N.M. – CRC Press, 1998. – 368 p.

14. Шелков А.Б. Аудит нформационной безопасности автоматизированных систем управления / А.Б. Шелков, В.Л. Шульц, В.В. Кульба // Тренды и управление. – 2014. – № 4. – С. 319-334.

15. Найханова И.В. Аудит систем менеджмента качества и информационной безопасности / И.В. Найханова // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. – 2011. – № SPEC. – С. 152-156.

16. Методы оценки несоответствия средств защиты информации / А.С. Марков, В.Л. Цирлов, А.В. Барабанов; под ред. А. С.Маркова. – М.: Радио и связь, 2012. – 192 с.

17. Петренко С.А. Аудит безопасности Intranet / С.А. Петренко, А.А. Петренко. – М.: ДМК Пресс, 2002. – 416 с.

18. Зеленский О.А. Построение математической модели для анализа и оценки уровня безопасности персональных данных в информационных системах / О.А. Зеленский // Вестник Московского университета имени С. Ю. Витте. – 2013. –№ 1 (2). – С. 83–87.

19. Поддержка принятия решений при стратегическом управлении предприятием на основе инженерии знаний / Л.Р. Черняховская, Е.Б. Старцева, П.В. Муксимов, К.А. Макаров, А.И. Малахова. – Уфа: АН РБ, Гилем, 2010. – 128 с.

20. Найханова И.В. Иерархическая структура показателей аудита безопасности персональных данных / И.В. Найханова // Глобальный научный потенциал. – 2014. – № 2(35). – С. 75-78.

21. Ярушкина Н.Г. Основы теории нечетких и гибридных систем: учеб. пособие / Н.Г. Ярушкина. – М.: Финансы и статистика, 2004. – 320 с.

Надійшла до редколегії 20.11.2015

Рецензент: д-р техн. наук, проф. О.В. Кувшинов, Військовий інститут телекомунікацій та інформатизації, Київ.

МЕТОДИКА АУДИТА ВТОРЖЕНИЙ В МОБИЛЬНЫЕ РАДИОСЕТИ КЛАССА MANET

С.В.Сальник, В.В.Сальник, Е.М.Бовда

В статье представлена методика аудита вторжений в мобильные радиосети класса MANET. Разработка методики основана на алгоритме действий, который включает в себя этапы и шаги проведения анализа, мониторинга данных и тестирования мобильной радиосети. Было предложено подход аудита, которой основывается на использовании нейронной сети с возможностью проведения самообучения, работе при нечеткой сетевой активности, в условиях режима реального времени и параметров, которыми характеризуется мобильная радиосеть. Разработана методика проведения аудита вторжений в мобильную радиосеть позволяет повысить эффективность предоставления управленческих решений, упростить процесс проведения анализа, мониторинга и тестирования сети, а также служить основой для разработки программного продукта для проведения аудита уровня безопасности мобильной радиосети. Определены дальнейшее направление работы, по построению нечеткой базы знаний, которая улучшит проведения аудита сети и повысит уровень безопасности мобильной радиосети.

Ключевые слова: *мобильные радиосети, MANET, аудит вторжений.*

METHODOLOGY OF AUDIT INTRUSIONS IN MOBILE RADIO NETWORKS CLASS MANET

S.V. Salnyk, V.V. Salnyk, E.N. Bovda

In the article presented methodology of audit intrusions in mobile radio networks class MANET. Development of methodology was based on the algorithm of actions, that includes for itself the stages and steps of realization of analysis, monitoring of data and testing of mobile radio network. It was offered approach realization of audit, is base on that the use of neural network with possibility of realization of self-training, to work with fuzzy network activity, in the conditions of the real-time and parameters that a mobile radio network is characterized mode. Development of methodology realization of audit Intrusion in a mobile radio network allows promoting efficiency grant of administrative decisions, simplifying the process realization of analysis, monitoring and testing of network, and also serving as basis for software product development for realization audit strength of mobile radio network security. Determined direction of the work to build a fuzzy knowledge base that would improve audit network and enhance the security level of the mobile radio network.

Keywords: *mobile radio network, MANET, audit intrusions.*