УДК 621.396

д.т.н. Міночкін А.І. (ВІТІ)
д.т.н. Сова О.Я. (ВІТІ)
Сальник С.В. (ВІТІ)
Марилів О.О. (ВІТІ)

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА РІВНІ ВУЗЛА ТА МЕРЕЖІ В МОБІЛЬНИХ РАДІОМЕРЕЖАХ КЛАСУ MANET

В статті представлено методику оцінки ефективності виявлення вторгнень на рівні вузла та мережі в МР класу MANET, яка ґрунтується на проведенні імітаційного моделювання та аналітичній оцінці методів виявлення вторгнень. Під час досліджень експериментальним шляхом були отримані дані та побудовані графіки залежностей, а також з`ясовано, що запропонована методика дозволяє спростити процес оцінки ефективності методів виявлення вторгнень.

***Миночкин А.И., Сова О.Я., Сальник С.В., Марылив Е.А. Методика оценки эффективности определения вторжений на уровне узла и сети в мобильных радиосетях класса MANET**. В статье представлена методика оценки эффективности определения вторжений вторгнень на уровне узла и сети в МР класса MANET, которая основана на проведении имитационного моделирования и аналитической оценки методов определения вторжений. Во время исследований экспериментальным путем были получены данные и построены графики зависимостей, а также установлено, что предложенная методика позволяет упростить процесс оценки эффективности методов определения вторжений.*

***A. Minochkin, O. Sova, S. Salnik, O. Maryliv, Methodology evaluation of the effectiveness of intrusion detection at the mobile node and network level in mobile radio networks class MANET.** The article presents a methodology for assessment the effectiveness of intrusion at the mobile node and network level in mobile radio networks of the MANET class, which is based on simulation modeling and analytical assessment of intrusion detection methods. During the research, data were obtained and curves of dependencies were plotted, and it was established that the proposed methodology makes it possible to simplify the process of assessment the efficiency of intrusion detection methods.*

***Ключові слова:** оцінка ефективності, мобільні радіомережі, MANET, методи виявлення вторгнень.*

Актуальність дослідження та постановка завдань. Організація ефективного управління мобільними радіомережами (МР), що відносяться до класу MANET (*Mobile Ad-Hoc Networks*) потребує вирішення множини завдань, одним з яких є забезпечення безпеки передачі даних. Зважаючи на особливості функціонування МР (зокрема, складність побудови, динамічна природа функціонування, децентралізованість та масштабованість), виникає необхідність реалізації підсистеми забезпечення безпеки (ПЗБ), робота якої потребує застосування відповідних методів та алгоритмів [1].

Аналіз останніх досліджень і публікацій. Питанню захисту безпеки в інформаційних системах та оцінки ефективності присвячено багато робіт. До авторів, які розглядали це питання відносяться: В.Ю. Гайкович, Ю.В. Демченко, В.В. Лебедєв, В.С. Міхалевич, А.Н. Назаров, А.С. Олексюк, В.К. Размахнін, Г.В. Фоменков, С. Шаньгин, Ю.В. Щеглов та інші. Однак основна частина запропонованих рішень щодо оцінки ефективності, орієнтовані на використання методів експертного оцінювання, які не враховують характеристичні особливості МР. Тому виникає завдання, яке полягає у застосуванні таких методик оцінки ефективності процесу виявлення вторгнень, які б відображали вплив особливостей функціонування МР на процеси передачі інформації та забезпечення її безпеки в радіомережах класу MANET [2 – 7].

У [2, 3] показано, що найбільшу загрозу для МР може завдати вторгнення та вплив противника на вразливості ПЗБ. Взагалі вразливість підсистеми забезпечення безпеки є характеристикою захищеності мережі, в свою чергу будь яка вразливість ПЗБ несе у собі загрозу здійснення впливу на мережу чи інформацію. Вплив у МР може бути реалізовано у вигляді атаки на окремі вузли мережі, компоненти та інформацію на рівнях мережевої моделі OSI (*Open Systems Interconnection*).

Враховуючи особливості побудови мережі, ПЗБ потребує багаторівневої структури забезпечення безпеки в МР на інформаційному, програмному та апаратному рівнях.

Основними завданнями ПЗБ повинні бути: прийняття рішення щодо обмеження впливу на МР, забезпечення безпеки мережі, виявлення вторгнень, блокування супротивника або окремого вузла мережі, підтримання безпечної роботи елементів МР [3].

Виконання вказаних завдань в підсистемі забезпечення безпеки покладається на систему виявлення вторгнень (СВВ), функціонування якої залежить від ефективної роботи методів виявлення вторгнень (МВВ), які становлять основу будь-якої СВВ. Саме тому актуальним залишається питання розробки нових та удосконалення існуючих МВВ для використання в МР класу MANET, а також проведення оцінки їх ефективності.

У зв'язку з цим, ***мета статті*** полягає в підвищенні показників оцінки ефективності виявлення вторгнень на рівні вузла та мережі в МР класу MANET.

Об`єктом дослідження є процес забезпечення безпеки інформації, яка передається в МР.

Предмет дослідження – методика оцінки ефективності виявлення вторгнень в МР класу MANET.

Виклад основного матеріалу. Аналіз існуючих сьогодні ПЗБ у мережах загального призначення показує, що їх побудова ґрунтується на застосуванні програмних та апаратних засобів, оцінка яких здійснюється на основі стандартів ISO/IEC 17799; ISO/IEC 15408; ISO 9126. Тому для визначення ефективності функціонування та технічних можливостей ПЗБ в МР доцільно використовувати вимоги зазначених стандартів з урахуванням зазначених вище особливостей МР.

Виходячи із вимог стандартів, ефективність функціонування ПЗБ залежить від множини взаємопов`язаних між собою критеріїв, таких як: продуктивність, часова ефективність, функціональна придатність, точність, захищеність, надійність, стійкість до відмов, зручність використання, здатність до співіснування та інші. Так як деякі критерії та характеристики ПЗБ, які вказані у різних стандартах, є взаємопов`язаними між собою, а деякі не відображають особливостей функціонування МР класу MANET, то в якості основних критеріїв оцінки ПЗБ доцільно визначити наступні: швидкість виявлення вторгнень, точність виявлення вторгнень, швидкість навчання МВВ [4].

Позначення вихідних даних: МР представлена у вигляді графа $G=(N,V)$, N – множина вузлів та $V=\{V_k\}, k=\overline{1,k}$ – множина потоків даних, таких що: $V_k=\{n_{pv}\cup n_{pb}\}$, де n_{pv} – кількість повідомлень з вторгненням, n_{pb} – кількість повідомлень без вторгнень; $X^k(t)=\{x^k{}_1(t),x^k{}_2(t),...,x^k{}_{41}(t)\}$ – 41 параметр, що описує вхідний трафік; $Q(t)$ – обсяг бази знань МВВ; $I(t)$ – множина ідентифікованих типів поведінок; $l(t)$ – кількість атакованих об`єктів; t_0 – початок проведення вторгнень.

Показники технічної ідентифікації:

– достовірність ідентифікації типу вторгнень $P_r=[(Q(t),I(t)),(k(t),M_{VV})]$;

– інтервал часу виявлення вторгнень $T=\max\{t_{kj}\}$,

де $t_{kj}=\begin{cases}t_{id}, \text{ якщо } I\in Q\\ t_{id}+t_{nav}, \text{якщо } I\notin Q\end{cases}$ – інтервал часу j-го виявлення вторгнень від k-го потоку даних; t_{id} – час ідентифікації поведінки; t_{nav} – час навчання МВВ.

Обмеження та допущення: Виявлення вторгнень відбувається на основі технічної ідентифікації параметрів трафіка. Ідентифікуються типи (*DoS, U2R, R2L, Probe*) атак. Аномальна поведінка ідентифікується, як нововиявлене вторгнення. Процес вторгнення є квазістаціонарним на інтервалі часу $(t_0...T)$.

Обмеження на процес технічної ідентифікації та ресурси:

$$\Omega'=\{P_r\geq P_{r\ isn},\ e_з\leq e_{з\max},F\leq F_{dop}\},\qquad(1)$$

де $P_{r\,isn}$ – достовірність виявлення вторгнень існуючими МВВ; $e_з$ – залишкова ємність батареї; F_{dop} – допустима продуктивність МВВ.

Необхідно: провести оцінку ефективності виявлення вторгнень МВВ [5, 6], де умовою є мінімізація інтервалу часу прийняття рішення на виявлення вторгнень,

$$U^*(t) = \arg \min_{U(t)\in\Omega} T(S(t);U(t)), \text{ де } S(t) = \{X^k(t);k(t)\}. \quad (2)$$

Методика оцінки ефективності МВВ в мобільні радіомережі класу MANET.

До особливостей впливу в МР відносять вторгнення, які відбуваються за допомогою множини різнонаправлених за своїм фізичним змістом атак на рівнях моделі OSI [7]. У цілому вплив атак в МР можливо умовно поділити на дві частини вузлову та мережеву.

В свою чергу СВВ з метою проведення ідентифікації вторгнень проводить аналіз мережевого трафіка, який складається з 41 параметру. Дані параметри отримуються блоком технічної ідентифікації на основі протоколів відповідних рівнів OSI. У [8 – 10] зазначено, що з метою зменшення обчислювального навантаження МВВ, та для більш ефективної ідентифікації вторгнень на рівнях моделі OSI, доцільно проводити поділ 41 параметру трафіка: на вузлову та мережеву частину; основну частину, статистичні ознаки, ознаки окремого з`єднання, додаткові ознаки та інше.

Далі вказаний 41 параметр поділяється на 15 та 18 параметрів, які відносяться до вузлової та мережевої частини мобільної радіомережі [5, 6, 10].

В свою чергу проведений аналіз [11 – 13] вказує на те, що вирішення завдання з проведення оцінки ефективності виявлення вторгнень на рівні вузла та мережі вимагає проведення імітаційного моделювання МВВ в основі якої перебуває гібридна структура МВВ яка складається з нейронних та нейрон-нечітких мереж, направлених на виявлення вторгнень на рівні вузла та мережі. Тому до етапів методики оцінки належать наступні:

I. ***Імітаційне моделювання процесу виявлення вторгнень в МР (ІМ).*** Шляхом проведення імітаційного моделювання МВВ на рівні вузла та мережі в середовищі MATLAB, експериментальним шляхом отримуються значення інтервалу часу виявлення вторгнень – T та достовірності ідентифікації типу вторгнень – P_r при різних умовах функціонування МВВ, які задаються параметрами (N , V). Структурна схема імітаційної моделі процесу виявлення вторгнень в МР з урахуванням МВВ зазначена на рис. 1.

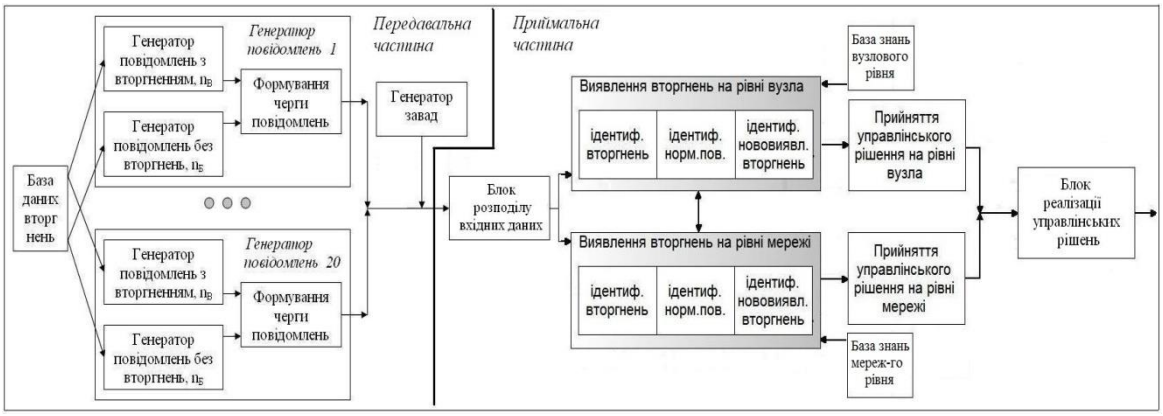

Рис. 1. Структурна схема імітаційної моделі процесу виявлення вторгнень в МР

З даної структурної схеми видно, що імітаційна модель складається з двох частин: передавальної та приймальної.

До передавальної частини належать 20 генераторів повідомлень, які імітують роботу 20-ти вузлів/станцій з яких надходять повідомлення. До складу генераторів повідомлень входять: блок-генератор повідомлень з вторгненням, блок-генератор повідомлень без вторгнень та блок формування черги повідомлень. Зазначені 20 генераторів повідомлень формують повідомлення користуючись базою даних вторгнень, яка містить параметри

трафіка аномального та нормального типів поведінки. Для імітації роботи МВВ за умов неповноти та нечіткості інформації в структурі імітаційної моделі міститься блок генератор завад, засобами якого буде імітовано невизначеності в МР, що виникають внаслідок її динамічної топології, непередбачуваності потоків даних, тощо.

До приймальної частини належать: блок розподілу даних на вузловий та мережевий МВВ; блоки виявлення вторгнень, у яких реалізовані методи виявлення вторгнень на рівні вузла та мережі; блоки баз знань для МВВ на вузловому та мережевому рівні; блоки прийняття управлінського рішення на рівні вузла та мережі; блок реалізації управлінського рішення. При побудові приймаючої частини імітаційної моделі доцільно врахувати характеристику існуючих засобів зв'язку. Тому, обробка даних, які забезпечують функціонування МВВ, здійснювалася з частотою 50 МГц, що відповідає процесорам типу DSP та ARM9, які використовуються при побудові сучасних радіозасобів.

В свою чергу процес виявлення вторгнень приймаючою частиною імітаційної моделі включає наступні етапи:

1. Етап – Отримання вхідних даних.

Приклад параметрів трафіка $X(t)=1,..,41$, (0,tcp,smtp,SF,829,327,0,0,0,0,0,1,0,0,0,0, 0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.0,0.00,0.00,8,113,0.88,0.25,0.12,0.02,0.00,0.00,0.00,0.00);

2. Етап – розподіл даних на вузловий та мережевий МВВ, $X(t)=\{X_V(t)\}\cup\{X_M(t)\}$;

3. Етап – ідентифікація – (*DoS, U2R, R2L, Probe*) атак та нормальної поведінки:

3.1. На рівні вузла $X_V(t)=\{x_b(t)\}$, $b=1,..,18$;

3.2. На рівні мережі $X_M(t)=\{x_m(t)\}$, $m=1,..,15$;

4. Етап – перевірка коректності ідентифікації:

Якщо U_{vt}=1 та U_{norm}=1 або U_{vt}=0 та U_{norm}=0, то U_{nov}=1;

5. Етап – прийняття управлінського рішення – $U(t)=\{u_{vt}\cup u_{norm}\cup u_{nov}\}$.

Структурна схема імітаційної моделі, виконаної в середовищі MATLAB, зображено на рис. 2 – 4.

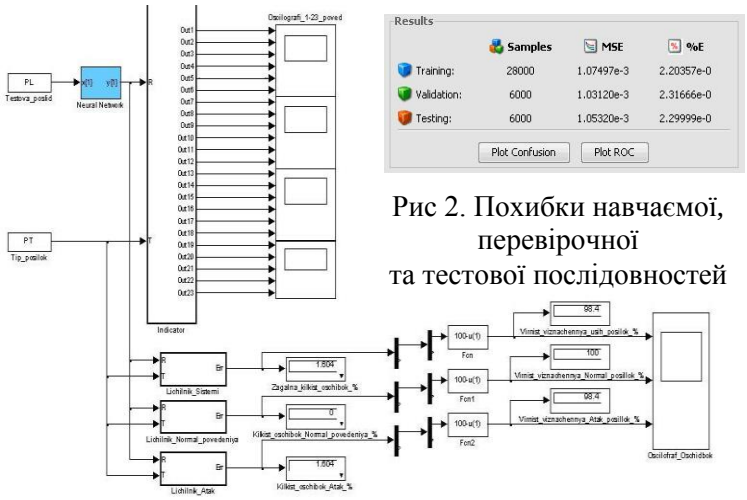

Рис 2. Похибки навчаємої, перевірочної та тестової послідовностей

Рис 3. Структурна схема ІМ

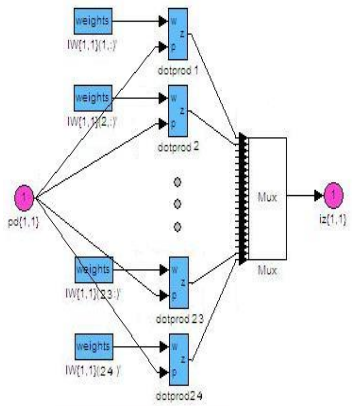

Рис 4. Структура НМ

ІІ. Оцінка ефективності виявлення вторгнень. Так як для рішення завдання оцінки ефективності виявлення вторгнень в МР необхідно враховувати не завжди відомі параметри, які являють собою незалежні змінні (регресори) та впливають на залежні змінні (критеріальні), у ролі яких виступають час виявлення вторгнень та достовірність виявлення вторгнень. В свою чергу оцінювання відбувається для визначення: значення залежної змінної за допомогою незалежної; внеску окремих незалежних змінних у варіацію залежної; ступеню відмінності значень критеріальної залежності залежної змінної від незалежної, то для оцінки

ефективності виявлення вторгнень в системах забезпечення безпеки доцільно застосовувати метод Найменших квадратів. За допомогою даного методу мінімізується сума квадратів відхилень деяких функцій, від пошукових змінних, які претендують на представлення регресійної залежності [14, 15].

В даному методі стохастична залежність між явищами описується, за допомого гіперболічної регресії:

$$\hat{y} = b_0 + b_1 \cdot \frac{1}{x}. \tag{3}$$

де b_0 – вирівнююча стала, яка відповідає точці перетину кривої регресії з віссю y; b_1 та b_2 – параметри регресії, яка характеризує залежність змінної y від змінної x.

Підбір функції відбувається виходячи із напрямку оцінки зв`язків між явищами. Тому для підрахунку оцінки ефективності МВВ в МР, у разі моделювання виявлення вторгнень на відрізку часу, доцільно використовувати гіперболічну функцію.

Нехай для опису залежності використовується гіперболічна форма зв`язку (3). При застосуванні методу Найменших квадратів до виразу (3), отримаємо систему рівнянь.

$$\sum y_i = b_0 m + b_1 \cdot \sum \frac{1}{x_i} \tag{4}$$

$$\sum y_i \frac{1}{x_i} = b_0 \sum \frac{1}{x_i} + b_1 \cdot \sum \frac{1}{(x_i)^2} \tag{5}$$

Вирішуючи їх, знаходимо b_0 та b_1:

$$b_0 = \frac{\sum y_i \sum \frac{1}{x_i^2} - \sum \frac{y_i}{x_i} \sum \frac{1}{x_i}}{m \sum \frac{1}{x_i^2} - \left(\sum \frac{1}{x_i} \right)^2} \tag{6}$$

$$b_1 = \frac{m \sum \frac{y_i}{x_i} - \sum \frac{1}{x_i} \sum y_i}{m \sum \frac{1}{x_i^2} - \left(\sum \frac{1}{x_i} \right)^2} \tag{7}$$

де m – відрізки часу проведення оцінювання.

За формулами (6) та (7) розраховуємо оцінку параметрів гіперболічного рівняння регресії, для МВВ та для кожного виду впливу типів вторгнень на об`єкти мережі. Після отримання оцінки параметрів при застосуванні виразу (3) будуємо відповідні графіки залежності. Оцінка середнього значення виявлення вторгнень МВВ наведена в таблиці 1.

Таблиця 1

Оцінка середнього значення виявлення вторгнень МВВ

Значення / Відрізки	X (сек.)	Y (P_r, %)	1/X	$1/X^2$	Y/X
1	1	88,75	1	1	88,75
2	5	89,5	0,2	0,04	17,9
3	10	90,5	0,1	0,01	9,05
4	15	91	0,066	0,0044	6,066
5	20	92	0,05	0,0025	4,6
6	25	93	0,04	0,0016	3,72
7	30	93,75	0,033	0,0011	3,125
8	35	94,75	0,028	0,0008	2,707
9	40	95	0,025	0,0006	2,375
10	45	96	0,022	0,0005	2,133
11	50	96,75	0,02	0,0004	1,935
12	55	97,25	0,018	0,0003	1,768
13	60	97,75	0,016	0,0003	1,629
Сума	391	1216	1,62	1,0625	145,759

– значення: b_0 = 94,38; b_1 = -6,77; t_{kj} = 177 мс; t_{nav} = 173 мс.

На графіках рис. 5 – 7 зображені результати оцінки ефективності виявлення вторгнень МВВМР [5, 6] на рівні вузла та мережі у вигляді залежностей достовірності виявлення вторгнень, часу навчання МВВ та часу виявлення вторгнення від кількості вузлів (потоків) при впливі на 1 об`єкт МР, який представлений 1 рівнем моделі OSI та відповідними йому протоколами. На графіках рис. 8 – 10 відображені результати оцінки ефективності виявлення вторгнень МВВМР [5, 6] на рівні вузла та мережі у вигляді залежностей достовірності виявлення вторгнень, часу навчання МВВ та часу виявлення вторгнення від кількості вузлів (потоків) при впливі на 7 об`єктів МР, які представлені 7 рівнями моделі OSI та відповідними протоколами для них протоколами.

З графіків видно, що при збільшенні кількості об`єктів на які відбувався вплив, значення оціночних показників змінюється у бік погіршення в наслідок збільшення обчислюваної складності ідентифікації вторгнень. Але значення оціночних показників удосконалених МВВМР [5, 6] мають виграш у порівнянні з існуючою системою виявлення вторгнень (IDS), а саме:

– достовірність виявлення вторгнень (рис. 5 та 8) удосконаленим МВВМР, в порівнянні з існуючою IDS, збільшується за рахунок застосування алгоритмів навчання та ідентифікації;

– час виявлення вторгнень (рис. 7 та 10) удосконаленим МВВМР, в порівнянні з існуючою IDS, зменшується за рахунок застосування алгоритмів ідентифікації вторгнень, які не використовуються в існуючих методах, та в наслідок зменшення часу навчання нейронної мережі;

– час навчання удосконаленого МВВМР (рис. 6 та 9), в порівнянні з існуючою IDS, зменшується за рахунок застосування алгоритмів ідентифікації та навчання, в наслідок чого в удосконаленому МВВ час навчання нейронної мережі попереднім вторгненням менший, ніж час виявлення наступного вторгнення.

В цілому вказана на графіках оцінка ефективності виявлення вторгнень демонструє менший час виявлення вторгнень та вищу достовірність виявлення вторгнень для удосконалених МВВМР в порівнянні з існуючої IDS, завдяки використанню розподілу множини різнорідних параметрів, застосуванні алгоритмів ідентифікації та навчання.

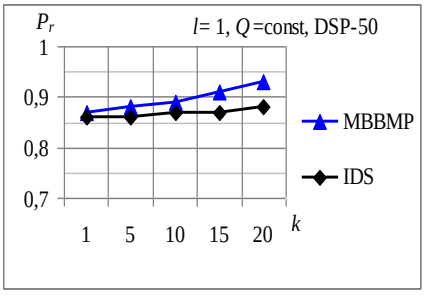

Рис. 5. Залежності достовірності виявлення вторгнень P_r від кількості вузлів (потоків даних) k

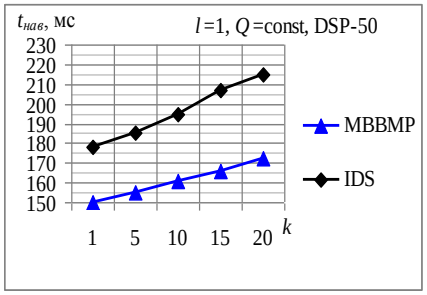

Рис. 6. Залежності часу навчання $t_{нав}$ від кількості вузлів (потоків даних) k

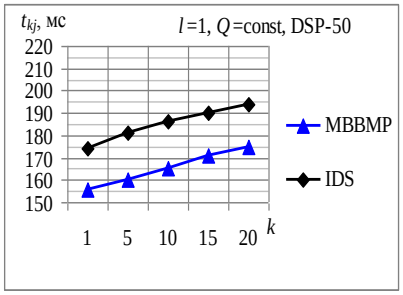

Рис. 7. Залежності часу виявлення вторгнень t_{jk} від кількості вузлів (потоків даних) k

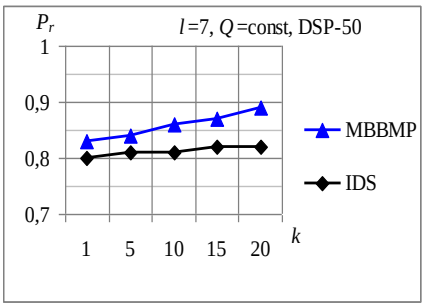

Рис 8. Залежності достовірності виявлення вторгнень P_r від кількості вузлів (потоків даних) k

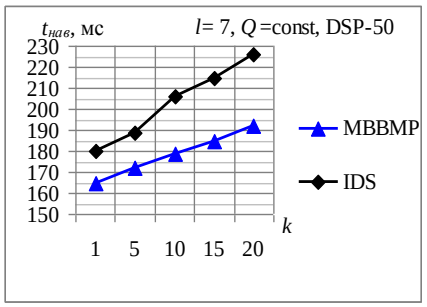

Рис 9. Залежності часу навчання $t_{нав}$ від кількості вузлів (потоків даних) k

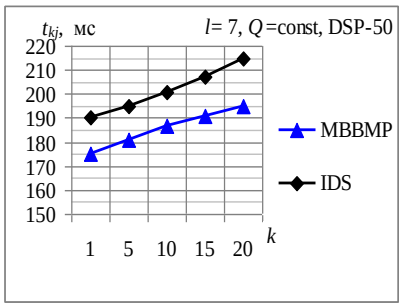

Рис 10. Залежності часу виявлення вторгнень t_{jk} від кількості вузлів (потоків даних) k

Оцінка ефективності виявлення вторгнень вказує на те, що на даному етапі розвитку інформаційних технологій розроблена методика є актуальною. Застосування даної методики до МВВМР [5, 6] свідчить про адекватність її розробки. В свою чергу етапи проведення

оцінки показують, що оцінка має структурований та поетапний характер. Дана методика може бути застосована для методів виявлення та запобігання вторгнень або слугувати основою для розробки методу оцінки рівня безпеки всієї МР.

Висновки. У статті представлена методика оцінки ефективності виявлення вторгнень на рівні вузла та мережі в МР класу MANET, яка основана на імітаційному моделюванні процесу виявлення вторгнень в МР. При застосуванні методики до МВВ зазначених в [5, 6], було зафіксовано зменшення часу виявлення вторгнень МВВМР в середньому на 15 – 20% при збереженні достовірності виявлення вторгнень на рівні не нижчому, ніж в існуючих системах виявлення вторгнень.

З метою підвищення ефективність функціонування методів виявлення та запобігання вторгнень в МР у ході подальших досліджень буде розроблено методику побудови баз знань для функціонування МВВ у МР класу MANET.

ЛІТЕРАТУРА

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

2. Миночкин А.И., Романюк В.А., Шацило П.В. Виявлення атак в мобільних радіомережах // Збірник наукових праць № 1. – К.: ВІТІ НТУУ „КПІ”.– 2005.– С. 102 – 111.

3. Сальник С.В., Сальник В.В., Сова О.Я., Стемпковська Я.А. / Модель вторгнень в мобільні радіомережі класу MANET // Журнал „Збірник наукових праць Харківського університету повітряних сил Збройних сил України”, № 1(46), – Харків: ХУПС імені І. Кожедуба – 2016 С. 79 – 85.

4. Сальник С.В., Сова О.Я., Міночкін Д.А. Аналіз методів виявлення вторгнень у мобільні радіомережі класу MANET // Журнал „Сучасні інформаційні технології у сфері безпеки та оборони” № 1(22)2015 – К.: НУОУ імені І. Черняховського – 2015. – С. 103 – 112.

5. Сальник С.В., Сальник В.В., Симоненко О.А., Сова О.Я. Метод виявлення вторгнень в мобільні радіомережі на основі нейронних мереж // Журнал „Наука і техніка повітряних сил ЗСУ” № 4(21)2015 – Харків: ХУПС імені І. Кожедуба – 2015. – С. 82 – 91.

6. Сальник С.В., Сальник В.В., Бовда Е.М., Міночкін Д.А. Метод виявлення вторгнень в мобільні радіомережі класу MANET на основі гібридного нейро-нечіткого класифікатора // Сучасні інформаційні технології у сфері безпеки та оборони. – 2016. – № 1. – С. 104 – 111.

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

8. Комар М.П., Палий И.О., Шевчук Р.П., Федисів Т.Б. Нейросетевой подход к обнаружению сетевых атак на компьютерные системы // Журнал „Інформатика та математичні методи в моделюванні” № Том 1, №2 – К – 2011. – С. 156 – 163.

9. Тимофеев А., Браницкий А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевых АТАК // International Journal „Information Technologies & Knowledge” Vol.6, Number 3,– 2012. – С. 257 – 265.

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

11. Альянах И.Н. Моделирование вычислительных систем / Альянах И.Н., – Л.: Машиностроение, 1988. – 223 с.

12. Петренко С.А., Симонов С.В. Управление информационными рисками: Экономически оправданная безопасность. – М.: АйТи – Пресс, 2004. – 381 с.

13. Чрешкин Д.С. Оценка эффективности систем защиты информацоионных ресурсов. – М.: Институт системного анализа РАН, 1998, – 455 с.

14. Калинина В.Н., Панкин В.Ф. Математическая статистика / – М.: Дрофа, 2002. – 336 с.

15. Линник Ю.В. Метод наименьших квадратов и основы математико-статистической теории обработки наблюдений / – М.: Государственное издательство Физико-математической литературы, 1958. – 336 с.