УДК 621.391

С. В. Сальник

МЕТОДИКА ОЦІНЮВАННЯ ФУНКЦІОНУВАННЯ ПІДСИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ РАДІОМЕРЕЖ КЛАСУ MANET

Представлено методику оцінювання функціонування підсистеми забезпечення безпеки мобільної радіомережі класу MANET. Розроблення методики ґрунтувалося на рішенні задачі оптимізації критеріїв оцінки ефективності, математичному та економічному оцінюванні. На їх основі отримані аналітичні вирази для оцінювання підсистеми забезпечення безпеки мобільної радіомережі.

Ключові слова: оцінювання функціонування, підсистема забезпечення безпеки, мобільні радіомережі, MANET.

Постановка проблеми. Організація управління мобільними радіомережами (МР) класу MANET (Mobile Ad-Hoc Networks) потребує виконання множини завдань, одним з яких є забезпечення безпеки передавання даних. Зважаючи на особливості функціонування МР, такі як мобільність, децентралізованість, масштабованість, динамічна природа функціонування, виникає необхідність реалізації підсистеми забезпечення безпеки (ПЗБ), робота якої передбачає застосування спеціалізованого обладнання, алгоритмів та методів [1].

У статті [2] показано, що найбільшу загрозу для МР може створити вторгнення противника у ПЗБ та вплив на них. У цілому характеристикою захищеності МР може бути вразливість ПЗБ. Її можливо реалізувати у вигляді атаки на окремі вузли мережі та інформацію на рівнях мережевої моделі OSI (Open Systems Interconnection), що своєю чергою несе у собі загрозу здійснення впливу на мережу чи інформацію.

Основними завданнями ПЗБ є: прийняття рішення з обмеження впливу на МР, забезпечення безпеки мережі, виявлення вторгнень, блокування вторгнення або окремого вузла мережі, підтримання безпечної роботи елементів МР. Виконання вказаних завдань залежить від ефективної дії відповідних методів, які складають основу ПЗБ. Саме тому актуальним залишається питання оцінювання функціонування ПЗБ у МР класу MANET [2, 3].

Мета статті. Розроблення методики оцінювання функціонування ПЗБ у МР класу MANET.

Виклад основного матеріалу. Питанню забезпечення безпеки в інформаційних системах та оцінюванню її ефективності присвячено багато праць. Його розглядали: В. Ю. Гайкович, Ю. В. Демченко, В. И. Завгородній, А. Г. Карпов, В. В. Лебедєв, В. С. Міхалевич, А. Н. Назаров, А. С. Олексюк, А. Ю. Першин, В. К. Размахнін, И. В. Сергиєнко, Ю. Я. Самохвалов, Г. В. Фоменков, С. Шаньгин, Ю. В. Щеглов та ін.

Однак у більшості запропонованих рішень щодо оцінювання функціонування не надано числових підходів до визначення рівня захищеності інформаційної системи. Оцінку зазвичай дають експерти з інформаційних технологій. Також важливим є розроблення підходів до оцінювання ефективності для середовищ, які не враховують характеристичні особливості МР. Отже, варто застосовувати підходи до оцінювання ПЗБ з урахуванням особливостей МР.

Будова сучасних ПЗБ ґрунтується на застосуванні програмних та апаратних засобів, які забезпечують безпеку МР. Тому для визначення ефективності рівня функціонування та технічних можливостей ПЗБ необхідно використовувати стандарти в галузі оцінювання характеристик їх якості. Найбільш відомими стандартами оцінювання захисту є ISO/IEC 17799, ISO/IEC 15408 та ISO 9126 [4].

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 ін. Однак наразі не існує загального підходу до визначення критеріїв оцінювання безпеки інформації, а в основу визначення критеріїв покладено множину завдань, які повинна виконувати ПЗБ.

Через те, що деякі критерії та характеристики ПЗБ, які вказані у стандартах, взаємопов'язані між собою, а деякі не відображають особливостей функціонування МР класу MANET, доцільно визначити як основні критерії оцінки ПЗБ такі: точність виявлення вторгнень, швидкість виявлення вторгнень, вартість функціонування ПЗБ [2]. Однак у даному випадку визначені критерії за своїм фізичним змістом не пов'язані між собою, а характеризують ті якості, які повинна мати ПЗБ, отже,

виникає необхідність розв'язування багатокритеріальної задачі оцінювання ПЗБ [4]. Своєю чергою проведення розрахунків з оцінювання функціонування ПЗБ покладатиметься на відповідні методи оцінювання (таблиця).

Т а б л и ц я

Методи оцінювання ефективності функціонування ПЗБ та їх особливості

Назва	Характеристика
метод Балаша	Призначений для рішення задач цілочислового програмування з булевими змінними. Недоліком методу є те, що процедура перебору передбачає дослідження усіх можливих наборів значень булевих змінних.
метод Монте-Карло	Ґрунтується на відтворенні множини реалізації випадкового процесу, побудованого за умовами завдання. Суть методу полягає у математичному моделюванні випадкових процесів, які мають місце в реальній системі. Недоліком методу є те, що через наявність великої кількості внутрішніх взаємозв'язків отримуємо нестійке рішення. Збільшення кількості розрахунків може негативно впливати на їх точність.
метод Алмон	Призначений для оцінювання коефіцієнтів моделі та застосовується до моделей, які характеризуються поліноміальною структурою лага і його кінцевим значенням. Метод застосовується у моделюванні процесів, які характеризуються різними структурами лагів. Недоліком методу є неможливість обчислювати статистичні коефіцієнти регресії при лагових змінних.
метод гілок і меж	Призначений для знаходження оптимальних рішень з відсівом підмножин можливих рішень, які не мають оптимальних рішень. Недоліком методу є необхідність оброблення великої кількості варіантів, перед тим як буде знайдено оптимальне рішення, а це впливає на час оцінювання.
метод Т. Сааті	Є багаторівневим експертним оцінюванням та методом ієрархічних процесів. Метод ґрунтується на принципі проведення парних порівнянь та обрахуванні вектора пріоритетності, який ранжують за відносною важливістю. Недолік методу в тому, що парні порівняння використовуються для отримання кількісного значення та критеріальних оцінок.
метод найменших квадратів	Оснований на мінімізації суми квадратів відхилень функцій від пошукових даних. Він застосовується для розв'язування широкого кола задач. Обчислення відбувається за рахунок механічної процедури знаходження коефіцієнтів і характеризується отриманням доступних математичних висновків. Недоліком методу є чутливість оцінок до швидкозмінюючихся даних.

Виходячи з характеристичних особливостей методів оцінювання та враховуючи вказане у працях [1–12], доцільно застосовувати метод найменших квадратів для оцінювання функціонування ПЗБ у МР.

Вихідними даними є: параметри моделювання впливу в МР: кількість відрізків часу, на яких відбувається оцінювання поточного стану виявлення вторгнень; відрізки часу, на яких відбувається оцінювання поточного стану виявлення вторгнень; відсоток виявлення вторгнень на відрізку часу; сумарна вартість ПЗБ; вартість захищаємої інформації; вартість об'єкта захисту інформації.

Обмеження та допущення. Кількість виявлених типів вторгнень в мережу обмежена навчальною вибіркою з бази даних KDD Cup 1999 Data. Навчальна вибірка має 20 % нормальних з'єднань та 80 % аномальних, які містять типи вторгнень [4, 5].

Для отримання повної картини функціонування ПЗБ та захищеності мережі необхідно врахувати об'єкти МР, які можуть бути атаковані. Тому реалізація варіантів вторгнення на об'єкт мережі може бути описана законом імовірності. До об'єктів, на які може поширитись дана ймовірність, можна віднести вплив окремого типу вторгнень (множини вторгнень) на окремий об'єкт мережі або множину об'єктів мережі.

Розв'язуючи багатокритеріальну задачу, виникає необхідність введення обмежень, пов'язаних з цільовими функціями (критеріями). А саме: точність виявлення вторгнень не може перевищувати 100 %; швидкість їх виявлення повинна постійно наближуватись до 0, але не може дорівнювати або бути менше 0.

Враховуючи викладене, процес оцінювання ПЗБ у МР класу MANET розділимо на два етапи.

Перший етап. Математичне оцінювання. Ймовірність вдалого вторгнення на N вузол мережі шляхом застосування j_z типів вторгнень має такий вигляд:

$$P_r = \max_j P_i^j,\ j = 1 \ldots j_z. \tag{1}$$

Для оцінювання ПЗБ у МР необхідно враховувати не завжди відомі параметри, які являють собою незалежні змінні (регресори) X_1, X_2, X_3 та впливають на залежні змінні (критеріальні) Y, якими є оціночні відрізки та відсоток виявлення вторгнень. Оскільки метою оцінювання є: 1) визначення значення залежної змінної за допомогою незалежної; 2) визначення внеску окремих незалежних змінних у варіацію залежної; 3) визначення ступеня відмінності значень критеріальної залежності залежної змінної від незалежної, то використовуємо метод найменших квадратів (МНК). За допомогою МНК мінімізується сума квадратів відхилень деяких функцій Y від пошукових змінних $\widehat{Y}$, які претендують на представлення регресійної залежності. МНК застосовується для оцінювання невідомих параметрів регресивних моделей за вибірковими даними [6, 7].

Сьогодні не існує універсального методу для вибору та обгрунтування типу кривої регресії. Тому одностороння стохастична залежність між явищами може бути описана, наприклад, за допомого поліноміальної регресії

$$\hat{y} = b_0 + b_1 x_1 + b_2 x_2 + \ldots, \tag{2}$$

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

Або за допомогою гіперболічної регресії:

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

Пам'ятаючи, що ПЗБ забезпечує безпеку МР, виходячи з її характеристичних особливостей, кожна оцінка включатиме в себе оцінку впливу вторгнень на об'єкти МР. Остання в середовищі з чіткою та нечіткою мережевою активністю поділяється на чотири оцінки [2, 9].

1. Виявлення окремого типу вторгнення на окремий об'єкт мережі. Ймовірність впливу варіантів проведення вторгнення z на окремий об'єкт мережі d:

$$P(z/d): z \to d. \tag{4}$$

2. Виявлення окремого типу вторгнення на множину об'єктів мережі. Ймовірність впливу варіантів проведення вторгнення z на множину об'єктів мережі d:

$$P(z/\sum d): z \to \sum d. \tag{5}$$

3. Виявлення множини типів вторгнень на окремий об'єкті мережі. Ймовірність впливу множини варіантів проведення вторгнення z на окремий об'єкті мережі d:

$$P(\sum z/d): \sum z \to d. \tag{6}$$

4. Виявлення множини типів вторгнень на множину об'єктів мережі. Ймовірність впливу множини варіантів проведення вторгнення z на множину об'єктів мережі d:

$$P(\sum z/\sum d): \sum z \to \sum d. \tag{7}$$

Ймовірність здійснення k вторгнень за час t буде розподілена за законом Пуассона. Отже, як гіпотезу закону розподілу вторгнення приймемо закон розподілу Пуассона. Значення вторгнень визначатиметься як

$$Y = \frac{1}{x}\sum_{i=1}^{x} y_i, \tag{8}$$

де y_i – значення випадкової величини на i-му відрізку часу; x – кількість інтервалів часу.

Враховуючи, що кожен вузол мережі містить систему виявлення вторгнень, ймовірність виявлення вторгнення цією системою буде визначатися формулою

$$P_B = \min_b P_i^b,\ b = 1 \ldots b_n. \tag{9}$$

Розглянуті вирази показують, що виявлення вторгнень в МР залежатиме від швидкості адаптації існуючих систем виявлення вторгнень до нових загроз. А рівень безпеки мережі залежить від вибору стратегії проведення вторгнення в МР [8].

Розв'язуючи задачу для декількох цільових функцій, де необхідно одночасно враховувати множину критеріїв, дійдемо до поняття ефективного (оптимального, за Парето) рішення з такою умовою. Нехай l є множина допустимих рішень у деякому завданні, а $l \in L$ – допустиме рішення. Покладемо, що кожне рішення $l \in L$ оцінюється за n критеріями.

Наразі відома ефективна конструкція для розв'язування подібних багатокритеріальних задач – поняття оптимального, за Парето, або ефективного рішення [4, 5]. Для цього сформулюємо необхідну умову оптимальності Парето.

Обмеження $g_i(l)$ у точці l^* називається активним, якщо $g_i(l^*) = 0$. Множину усіх активних обмежень $\left\{ i \in 1,...,k \;\middle|\; g_i(l^*) = 0 \right\}$ позначимо $A(l^*)$.

Якщо точка l^* є локальною парето-оптимальною для значення багатокритеріальної оптимізації, то система

$$\left(\nabla f_i(l^*)\right)^T \nu < 0, \quad i = 1,...,k, \quad \nu \in T_\Omega(l) \;, \tag{10}$$

де ν – вектор коефіцієнтів з бази розв'язків, не матиме рішення.

Точка, в якій виконані умови локальної парето-оптимальності, буде критичною. Рішення $l^* \in L$ буде парето-оптимальним (ефективним), якщо не існує іншого рішення $l \in L$, для якого $H_i(l) \geq H_i(l^*), i = \overline{1,n}, \; \exists i_0 : H_{i_0}(l) > H_{i_0}(l^*)$ [4, 5].

Другий етап. Економічне оцінювання ПЗБ. Оцінювання використання ПЗБ у МР класу MANET ґрунтується на співвідношенні корисних результатів її функціонування до використаних ресурсів на її побудову [10]. Основним показником ефективності ПЗБ є коефіцієнт ефективності $K_{эф}$ як показник її наближення до граничних затрат на побудову ПЗБ:

$$K_{еф} = \frac{S_{MBB}}{M_{MBB}}, \tag{11}$$

де S_{MBB} – сумарна вартість ПЗБ; M_{MBB} – граничні витрати на ПЗБ.

Таким чином, найбільш ефективним буде ПЗБ, в якій за найменших витрат на її побудову необхідні найбільші витрати на вторгнення до неї, а також виконуються такі умови [11, 12]:

$$\begin{cases} S_{MBB} \leq \Delta R_I + \Delta R_{OI} + \Delta R_{MBB}; \\ S_{MBB} \leq S_I + S_{OI}, \end{cases} \tag{12}$$

де $\Delta R_I + \Delta R_{OI} + \Delta R_{MBB}$ – загальне зниження ризиків для ПЗБ; S_I – вартість захищаємої інформації; S_{OI} – вартість захищаємого об'єкта інформації; S_{MBB} – сумарна вартість ПЗБ; R_I – сумарний ризик інформації; R_{OI} – сумарний ризик об'єкта інформації; R_{MBB} – сумарний ризик ПЗБ.

Вартість інформації U рівня обмеження доступу, що передається на n рівні моделі OSI, розраховується так:

$$S_{nu} = S_{u0} \cdot V_{nU}, \tag{13}$$

де S_{u0} – вартість одиниці обсягу інформації u категорії важливості; V_{nU} – обсяг інформації u категорії важливості, що передається на n рівні моделі OSI.

З'ясуємо обсяг V_Σ та вартість S_Σ інформаційної, програмної або апаратної складової, яка потребує захисту та передається на n рівні моделі OSI.

$$V_\Sigma = \sum_{n=1}^{N} V_n \;, \tag{14}$$

$$S_\Sigma = \sum_{n=1}^{N} S_n \;, \tag{15}$$

де N – кількість рівнів моделі OSI.

Таким чином, коефіцієнт впливу відповідає відношенню

$$\alpha_n = \frac{S_n}{S_\Sigma}, \tag{16}$$

де α_n – частина впливу, який може бути задіяний на n рівні моделі OSI [11, 12].

Після визначення вартості інформації та ПЗБ потрібно врахувати перелік вторгнень, які можуть бути реалізовані. У математичному вигляді він представляє собою матрицю вторгнень та складових ПЗБ розмірністю $n \times m$, де n – рівні моделі OSI, m – типи вторгнень. Тому для кожного i вторгнення по відношенню до j рівня моделі OSI визначається ймовірність реалізації p_{rij}.

Для кожного рівня розраховується реалізація хоча б одного вторгнення:

$$p_{ri} = 1 - \prod_{i=1}^{n}(1 - p_{rij}). \quad (17)$$

У даному випадку мається на увазі, що у випадку реалізації j рівня моделі OSI хоча б одним вторгненням, збиток дорівнюватиме вартості рівня моделі OSI.

$$q_j = s_j. \quad (18)$$

Вартість вторгнення для кожного рівня моделі OSI дорівнює

$$R_j = p_{rj} \cdot q_j. \quad (19)$$

Вартість повного вторгнення дорівнює сумі вторгнень на всі рівні моделі OSI

$$R_{П} = \sum_{j=1}^{m} R_j. \quad (20)$$

Також потрібно врахувати роботу ПЗБ, яка призначена для виявлення вторгнення. Тому остаточна вартість вторгнення R_O буде менша за повну вартість. У даному випадку значення S_{MBB} (сумарна вартість ПЗБ) відповідатиме значенню $R_{П} - R_O$.

Отже, коефіцієнт економічної ефективності матиме такий вигляд:

$$K_{еф} = \frac{R_{П} - R_O}{M_{MBB}}. \quad (21)$$

Отримане значення $K_{еф} > 1$ свідчитиме про ефективність ПЗБ, у іншому випадку – про її неефективність [12].

На даному етапі розвитку інформаційних технологій розроблена методика оцінювання є актуальною. Оцінювання мережі має структурований та поетапний характер. Воно може бути застосоване для виявлення та запобігання вторгненням або слугувати основою для розроблення методу оцінювання рівня безпеки всієї МР.

Висновки

Представлено методику оцінювання функціонування ПЗБ у МР класу MANET, яка основана на вирішенні багатокритеріальної задачі оптимізації цільових функцій, оцінюванні ефективності функціонування, математичному та економічному оцінюванні. Запропонована методика ґрунтується на можливості окремого оцінювання роботи ПЗБ з урахуванням варіантів впливу типів вторгнення на об’єкти мережі, дозволяє значно спростити оцінювання методів, що забезпечують роботу ПЗБ у МР. У ході подальших досліджень буде розроблено метод оцінювання ефективності методів виявлення вторгнень в МР класу MANET та застосовано його до розроблених методів виявлення вторгнень.

Список використаних джерел

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

2. Метод виявлення вторгнень в мобільні радіомережі на основі нейронних мереж [Текст] / 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.

3. Миночкин, А. І. Виявлення атак в мобільних радіомережах [Текст] / А. І. Миночкин, В. А. Романюк, П. В. Шацило // Збірник наукових праць № 1. – К. : ВІТІ НТУУ “КПІ”, 2005. – С. 102–111.

4. Подиновский, В. В. Парето-оптимальные решения многокритериальных задач [Текст] / В. В. Подиновский, В. Д. Ногин. – М. : Наука, 1982. – 64 с.

5. Лотов, В. А. Многокритериальные задачи принятия решений [Текст] : учеб. пособие / В. А. Лотов, И. И. Поспелова. – М. : МАКС Пресс, 2008. – 197 с.

6. Зорич, В. А. Математический анализ [Текст]. Ч. I / В. А. Зорич. – Изд. 4-е, испр. – М. : МЦНМО, 2002. – 664 с.

7. Зорич, В. А. Математический анализ [Текст]. Ч. II / В. А. Зорич. – Изд. 4-е, испр. – М. : МЦНМО, 2002. – 794 с.

8. Модель вторгнень в мобільні радіомережі класу MANET [Текст] / С. В. Сальник, В. В. Сальник, О. Я. Сова, Я. А. Стемпковська // Збірник наукових праць Харківського університету Повітряних Сил Збройних Сил України імені І. Кожедуба. – Х. : ХУПС імені І. Кожедуба, 2016. – № 1 (46). – С. 79–85.

9. Сальник, С. В. Методика аудиту вторгнень в мобільні радіомережі класу MANET [Текст] / С. В. Сальник, В. В. Сальник, Е. М. Бовда // Журнал ХУПС імені І. Кожедуба "Системи обробки інформації". – 2016. – № 1 (138). – С. 125–131.

10. Альянах, И. Н. Моделирование вычислительных систем [Текст] / И. Н. Альянах. – Л. : Машиностроение, 1988. – 223 с.

11. Петренко, С. А. Управление информационными рисками: Экономически оправданная безопасность [Текст] / С. А. Петренко, С. В. Симонов. – М. : АйТи-Пресс, 2004. – 381 с.

12. Чрешкин, Д. С. Оценка эффективности систем защиты информацоионных ресурсов [Текст] / Д. С. Чрешкин. – М. : Ин-т системного анализа РАН, 1998. – 455 с.

Стаття надійшла до редакції 23.03.2016 р.

УДК 621.391

С. В. Сальник

МЕТОДИКА ОЦЕНКИ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МОБИЛЬНЫХ РАДИОСЕТЕЙ КЛАССА MANET

Представлена методика оценки функционирования подсистемы обеспечения безопасности мобильной радиосети класса MANET. Разработка методики основывалась на решении задачи оптимизации критериев оценки эффективности, математической и экономической оценке. На их основе получены аналитические выражения для оценивания подсистемы обеспечения безопасности мобильной радиосети.

К л ю ч е в ы е с л о в а: оценка функционирования, подсистема обеспечения безопасности, мобильные радиосети, MANET.

UDC 621.391

S. V. Salnik

METHODOLOGY ESTIMATION FUNCTIONING OF SUBSYSTEM PROVIDING SAFETY OF MOBILE RADIO NETWORKS CLASS MANET

In article the presented methodology estimation functioning of subsystem providing safety of mobile radio network class MANET. Development methodology was base on decision task optimization criteria estimation efficiency mathematical estimations and economic estimations. On basis indicated analytical expressions were got for estimation subsystem providing safety of mobile radio network.

K e y w o r d s: estimation functioning, subsystem providing safety, mobile radio networks, MANET.

Сальник Сергій Васильович – ад'юнкт Військового інституту телекомунікацій та інформатизації