УДК 621.391

С.В. Сальник, В.В. Сальник, О.Я. Сова, Я.А. Стемпковська

Військовий інститут телекомунікацій та інформатизації, Київ

МОДЕЛЬ ВТОРГНЕНЬ В МОБІЛЬНІ РАДІОМЕРЕЖІ КЛАСУ MANET

В статті представлена модель вторгнень в мобільні радіомережі класу MANET. Розробка моделі базувалася на множині вразливостей мобільної радіомережі, на які можливо впливати за допомогою атак. Було розглянуто перелік загроз безпеці мобільної радіомережі, види застосовуваних атак на рівнях мережевої моделі OSI, приклади реалізації атак та варіанти впливу на мережу, що надало уявлення про можливості противника при впливі на мобільну радіомережу. На основі вказаного були отримані аналітичні вирази для оцінки ймовірності реалізації ризиків та ймовірностей порушення безпеки мобільної радіомережі на рівнях мережевої моделі OSI. Використання отриманої моделі загроз дає можливість для проведення прогнозування вторгнень противника та моделювання наслідків вторгнення в режимі реального часу.

Ключові слова: *мобільні радіомережі, MANET, вторгнення в мобільну радіомережу*.

Вступ

Аналіз предметної області. У зв`язку з тим, що система виявлення вторгнень (СВВ) потрібно виявляти вторгнення, у мобільні радіомережі (МР) та у систему управління нею [4, 5], то СВВ повинна відслідковувати весь трафік, що циркулює в МР. Для цього СВВ забезпечує своє функціонування на всіх рівнях моделі OSI, здійснюючи при цьому: контроль з`єднань, аналіз структури та вмісту мережевих пакетів, контроль трафіка та інше. При використанні МР в тактичній ланці управління військами, метою несанкціонованого доступу може бути приховане управління вузловими та мережевими ресурсами або вплив на інформаційні, програмні та апаратні засоби МР. Реалізація вказаної мети досягається за допомогою методів, які направлені на вразливості МР. В свою чергу це може призвести до віддаленого керування вузлом або його захоплення [7].

Під вразливістю розуміються властивості МР (архітектурний або інший недолік), які можуть бути використані для здійснення доступу до мережі, що робить можливим виникнення загрози вторгнення. В свою чергу вразливість являє собою характеристику захищеності мережі, а будь-яка вразливість мережі несе в собі загрозу впливу на мережу за допомогою атаки [6].

Мета атаки може не збігатися з метою загрози, та може бути спрямована на отримання проміжного результату необхідного для подальшої реалізації загрози. У разі такої невідповідності атака розглядається, як етап підготовки до вчинення дій, спрямованих на реалізацію загрози. Результатом атаки є наслідки які реалізувалися за допомогою загрози або сприяли такій реалізації [8].

Питання реалізації загроз та класифікація загроз безпеки в МР розглядалися в [2 – 4, 9 – 11], де зазначалося, що в ході вторгнення в мережу загроза проводиться за допомогою атаки, яка направлена на МР. Множина загроз безпеки МР при вторгненні в мережу зазначена на рис. 1.

Вказані загрози впливають на мережу та її компоненти, які забезпечують передачу інформації у відповідності з функціональними особливостями кожного об`єкта мережі.

Загроза реалізується на всіх рівнях мережевої моделі OSI та може впливати ззовні на об`єкт мережі (потік даних, вузол зв`язку, ретранслятор, кінцевий пристрій), а також із середини (трафік даних, програмно-апаратну частину мобільної або стаціонарної мережі).

В свою чергу вторгнення реалізовується множиною способів (вплив загрози на один чи декілька об`єктів; множина загроз на один об`єкт чи декілька об`єктів). Вказані способи направлені на досягнення проміжної або кінцевої мети, в наслідок чого відбувається: відмова в обслуговуванні, віддалене контролювання, блокування або захоплення частини мережі або МР в цілому [4, 12].

Розглядаючи практичне здійснення вторгнень (атак) на інформаційні, програмні та апаратні засоби МР, варто зазначити, що об'єктами атак є правила і технічні процедури, які здійснюють з'єднання і обмін даними в мережі, та відносяться до різних рівнів мережевої моделі OSI. Види впливу атак, які можуть бути застосовані на різних рівнях мережевої моделі OSI, наведено в табл. 1.

Перелік атак, які застосовуються для проведення вторгнень в МР поділяються на 4 категорії. Кожна з категорій містить множину типів атак, які використовуються для реалізації мети вторгнення. В свою чергу кожен тип атаки несе загрозу мережі на відповідних рівнях мережевої моделі OSI та виконує свою функцію, щодо здійснення деструктивного впливу на мережу [4, 10, 13]. До вказаних категорій атак відносять:

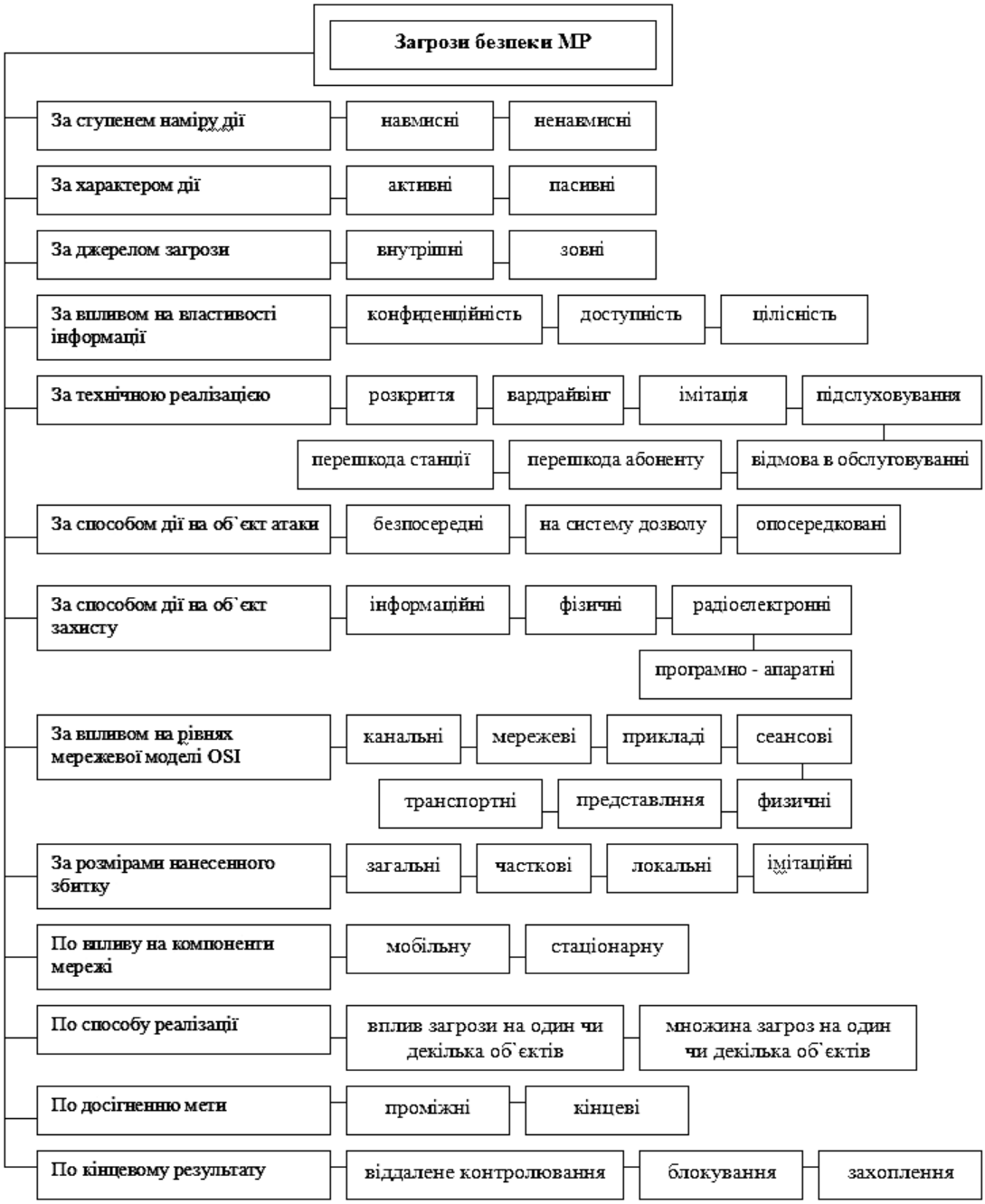

Рис. 1. Множина загроз безпеки МР при вторгненні в мережу

Таблиця 1

Види впливу атак на рівнях мережевої моделі OSI

Рівень моделі	Вплив атак
Прикладний рівень (Application)	Відмова в доступі до прикладних програм; отримання (або зміна) пріоритету обслуговування окремих видів трафіка, відмова в обслуговуванні, відмова у сервісі, порушення з`єднання мережі
Транспортний рівень (Transport)	Порушення доставки великих пакетів даних, побудова фальшивих пекетів, переповнення буферу, порушення в обслуговуванні шляхом частої відправки запитів, надсилання великої кількості пакетів запитів
Мережевий рівень (Network)	Порушення доставки повідомлень, порумення маршрутизації відмова в обслуговуванні певного класу трафіка, надсилання неправдивих повідомлень, атака ICMP-запитами, підроблення адрес
Канальний рівень (Data Link)	Порушення синхронізації, відмова в доступі, відмова в сервісі підтримка MAC-адреси, самостійна розсилка даних
Фізичний рівень (Physical)	Відмова в сервісі, розрив зв`язку, встановлення шуму, відмова у перетворенні сигналів, перехоплення та прослуховування

– DoS атаки – це мережеві атаки, спрямовані на виникнення ситуацій, коли у системі, що піддається вторгненню, відбувається відмова в обслуговуванні. Вказані атаки характеризуються генерацією великого об`єму трафіка, що призводить до перенавантаження та блокування сервера. До найчастіше застосованих DoS атак належать: back, land, neptune, pod, smurf, teardrop атаки.

– U2R атаки – пропонують отримання зареєстрованим користувачам привілей локального суперкористувача (мережевого адміністратора). До U2R атак відносять наступні типи атак: buffer_overflow, loadmodule, perl, rootkit.

– R2L атаки, що характеризуються отриманням доступу незареєстрованого користувача до мережі з боку віддаленої станції. Поділяють R2L атаки на: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster та інші атаки.

– Probe-атаки – полягають в скануванні мережевих портів з метою отримання конфіденційної інформації. Probe-атак поділяються на наступні типи: ipsweep, nmap, portsweep, satan та інші.

Вказані типи атак за своєю функцією можуть впливати на: управління передачею даних, обмін пакетами, організацію з'єднань, міжмережевий обмін, енергетичні характеристики засобів зв'язку, доступ до кодування, управління інформацією та інше.

Вплив вказаних категорій атак на рівнях мережевої моделі OSI [2-4,13], наведено в табл. 2.

Таблиця 2

Вплив атак на рівнях мережевої моделі OSI

Категорії атак	Типи атак	Рівні мережевої моделі OSI				
		Прикладний	Транспортний	Мережевий	Канальний	Фізичний
DoS	back	+	+	+	+	+
	land	+	+	+	+	+
	neptune		+	+		
	pod		+	+	+	+
	smurf			+	+	+
	teardrop	+	+	+	+	+
U2R	buffer_ overflow		+	+		+
	loadmodule		+	+		+
	perl	+	+	+		+
	rootkit	+	+	+	+	
R2L	ftp_write	+			+	
	guess_passwd	+	+		+	
	imap	+	+		+	
	multihop	+		+		+
	phf	+	+			
	spy	+			+	
	warezclient	+			+	+
	warezmaster	+				+
Probe	ipsweep			+	+	
	nmap			+	+	
	portsweep		+	+		
	satan	+		+		

На підставі викладеного, враховуючі: множину способів впливу на МР; сукупність елементів системи зв`язку, яка впливає на систему або на яку впливають, та з метою оцінки ймовірності реалізації вторгнень в мережу, та порушення нормального функціонування мережі визначимо:

метою статті є проведення оцінки ризиків здійснення вторгнення в МР на різних рівнях моделі OSI та отримання аналітичних виразів моделі вторгнень в МР;

об'єктом розгляду даної статті є процес забезпечення безпеки інформації, яка передається в МР;

предметом дослідження є модель вторгнень в МР класу MANET.

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 систему виявлення вторгнень [3,7], робить актуальним питання проведення моделювання вторгнень в мережу з метою забезпечення безпеки МР.

Результати досліджень

Позначення вихідних даних. Показники реалізації вторгнень в МР залежать від: кваліфікації того хто реалізує вторгнення, обладнання яке застосовується для здійснення вторгнення, покладених задач, стратегії здійснення вторгнення та інше. Противник в свою чергу розраховує на вразливості об'єкту вторгнення та низький рівень забезпечення безпеки МР. Також противник має множину інструментів (атак), для здійснення вторгнення, які в свою чергу впливатимуть на ймовірність успішного проведення вторгнення в МР.

Обмеження та допущення: Припустимо, що МР складається з N вузлів мережі, на які може впливати противник за допомогою множини типів вторгнень. Така множина типів вторгнень направлена на вразливості мережі та може бути реалізована на прикладному, транспортному, мережевому, канальному, фізичному рівнях. В свою чергу множина типів вторгнень направлена на вразливості мережі складає $Z = \{z_1, ..., z_n\}$ – множину варіантів проведення вторгнень. Ймовірність вторгнення в мережу за час t залежить від частоти вторгнень λ.

Кожен з N вузлів мережі містить СВВ навчену виявленню вторгнень, що являє собою $B = \{b_1, ..., b_n\}$ – множину варіантів виявлення вторгнень.

Необхідно: розробити модель вторгнень в МР класу MANET, для оцінки ймовірності реалізації певних порушень безпеки МР на рівнях моделі OSI.

Так як МР працює на всіх рівнях моделі OSI, а вразливості мережі до яких можуть бути застосовані типи вторгнень можуть бути рівнозначними для всіх рівнів мережі, то доцільно провести визначення ймовірностей вторгнення, як для типових значень на всіх рівнях моделі OSI. Разом з цим кожний рівень OSI матиме власне значення коефіцієнту вторгнення, виходячи із: кількості типів атак, які мають вплив на окремий рівень OSI; статистичних даних щодо впливу на кожен окремий рівень; можливостей СВВ щодо виявлення вторгнень та інше.

Виходячи із вказаного значення ймовірності вторгнення на окремому рівні моделі OSI в загальному вигляді матиме вигляд:

$$R = P_Z \cdot P_V \cdot \varpi, \qquad (1)$$

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.

Як наслідок, ймовірність того, що мережа на окремому рівні моделі OSI при використанні СВВ може бути застосована до виявлення j_Z типів вторгнень, у разі реалізації варіантів проведення вторгнень Z, де $z = 1, ..., Z$, буде визначатися:

$$P_a = 1 - \prod_{z=1}^{Z} \left(1 - P_{j_Z}\right). \qquad (2)$$

Так як варіанти проведення вторгнень z можуть бути реалізовано j_Z типами вторгнень, то існування джерела проведення вторгнення z визначається апріорною ймовірністю $\pi(z)$. В свою чергу реалізація варіантів проведення вторгнень z типами вторгнень j_Z визначатиметься ймовірністю $P(j_Z / z)$.

Тоді ймовірність реалізації варіантів проведення вторгнень на окремому рівні моделі OSI типами вторгнень j_Z від джерела вторгнень матиме вигляд:

$$P_Z = \pi(z) P(j_Z / z). \qquad (3)$$

Ймовірність вторгнення на окремому рівні моделі OSI за деякий час t, може здійснитися j_Z типами вторгнень з деякою частотою λ. З цього виходить, що час t доцільно розподілити на x рівних частин.

Тоді ймовірність того, що на відрізку часу відбудеться вторгнення визначатиметься:

$$P_t = \lambda t / x. \qquad (4)$$

В свою чергу на окремому рівні моделі OSI ймовірність того, що серед x рівних частин часу відбудеться j_Z типів вторгнень буде визначатися:

$$p_{j_Z}(t) = \left(\frac{\lambda t}{x}\right)^{j_Z} \left(1 - \frac{\lambda t}{x}\right)^{x - j_Z}. \qquad (5)$$

Для отримання повної картини захищеності мережі на окремому рівні моделі OSI необхідно врахувати об`єкти МР, які можуть бути атаковані. Тому реалізація варіантів проведення вторгнення $z$ на об`єкт мережі l може бути описано законом ймовірності.

До об`єктів на які може поширитись дана ймовірність можливо віднести:

$P(z / l)$ - ймовірність впливу варіантів проведення вторгнення z на окремий об`єкт мережі l;

$P(z / \sum l)$ - ймовірність впливу варіантів проведення вторгнення z на множину об`єктів мережі l;

$P(\sum z / l)$ - ймовірність впливу множини варіантів проведення вторгнення z на окремий об`єкті мережі l;

$P(\sum z / \sum l)$ - ймовірність впливу множини варіантів проведення вторгнення z на множину об`єктів мережі l.

Тобто:

$$P(z/l): z \to l; \quad (6)$$

$$P(z/\sum l): z \to \sum l; \quad (7)$$

$$P(\sum z/l): \sum z \to l; \quad (8)$$

$$P(\sum z/\sum l): \sum z \to \sum l. \quad (9)$$

Виходячи із вказаного ймовірність здійснення j_z типів вторгнень на множину об'єктів мережі l буде обчислюватись:

$$P(j_z, l) = \prod_{i=l}^{l} P_i^{j_z}. \quad (10)$$

Ймовірність здійснення вдалого вторгнення на окремому рівні моделі OSI, визначатиметься ймовірністю того, що вторгнення буде проведено на відрізку часу $1/t$. Відповідно до закону Пуасона буде отримано вираз:

$$P_k = 1 - e^{-\lambda/t}. \quad (11)$$

Враховуючі множину варіантів проведення вторгнень у мережу на окремому рівні мережевої моделі OSI, для представлення повної моделі вторгнень доцільно розглянути ймовірності здійснення вторгнення на L рівні моделі OSI та ймовірність вторгнень у МР в цілому.

Загальна оцінка мінімального часу, протягом якого відбувається вторгнення на рівні моделі OSI визначатиметься:

$$P(\min_t \sum_{j \in R(i)} \zeta_j\langle t) = $$

$$= 1 - \int_{\substack{x_i \ldots x_N \\ \sum_{j \in R(i)} x_j \geq t_i \forall_i}} \ldots \int \prod_j f_j(x_j) \cdot dx_1 \cdot \ldots \cdot dx_N. \quad (12)$$

Розглядаючи ймовірність вторгнень у МР в цілому потрібно врахувати вищевказане.

Ймовірність здійснення вдалого вторгнення на N вузол мережі шляхом застосування j_z типів вторгнень мати вигляд:

$$P_r = \max_j P_i^j,\ j = 1 \ldots j_z, \quad (13)$$

де P_i^j – ймовірність здійснення j_z типів вторгнень на i вузол.

Якщо $k(t)$ – частина вдало атакованих N вузлів, j_z типами вторгнень, то кожен такий вузол несе ймовірність скоєння $j_z(1 - j_z(t))$ нових вдалих вторгнень на інші вузли.

Таким чином, кількість атакованих вузлів за відрізок часу буде відповідати:

$$n = j_z N \cdot K(1 - j_z)dt. \quad (14)$$

У разі якщо кількість вузлів N в мережі буде постійним, то отримаємо:

$$n = d(j_z N) = N dj_z. \quad (15)$$

З урахуванням загального часу покладемо константу $C - \text{const}$, $C = -KT$.

Тоді вигляд матиме вираз:

$$\int \left(\frac{1}{j_z} + \frac{1}{1 - j_z} \right) \cdot dj_z = K \cdot t - KT. \quad (16)$$

Даний вираз в свою чергу матиме наступне рішення:

$$j_z = \frac{e^{K(t-T)}}{1 + e^{K(t-T)}}, \quad (17)$$

де T – часовий параметр, який характеризує найбільшу кількість вторгнень.

Ймовірність здійснення k вторгнень за час t буде розподілена за законом Пуассона. Отже, в якості гіпотези закону розподілу вторгнення, приймемо закон розподілу Пуассона, а середнє значення вторгнень визначатиметься:

$$Y = \frac{1}{x} \sum_{i=1}^{x} y_i, \quad (18)$$

де y_i – значення випадкової величини на i-ому відрізку часу при x – кількості інтервалів часу.

З можливим відхиленням:

$$\sigma \approx \frac{S_y}{\sqrt{x}} = \sqrt{\frac{1}{[(x-1)} \sum_{i=1}^{x} (y_i - Y)^2} = S_y, \quad (19)$$

де S_y - помилка середнього значення:

Перевірка гіпотези про розподілення випадкової величини, «кількість вторгнень на відрізку часу», за законом Пуассона [14], здійснюється за допомогою критерію згоди Пірсона за виразом:

$$F = \sum_{i=1}^{k} \frac{(m_i - x\lambda_i)^2}{x\lambda_i}, \quad (20)$$

де $\lambda_i = \frac{m_i}{x}$ – частота вторгнень на відрізку часу; m_i – кількість випадків з i-тою кількістю вторгнень на відрізку часу.

Враховуючі те, що кожен вузол мережі містить СВВ навчених виявленню вторгнень, то ймовірність виявлення вторгнення СВВ буде визначатися:

$$P_B = \min_b P_i^b,\ b = 1 \ldots b_n, \quad (21)$$

Розглянуті вирази, свідчать про те, що виявлення вторгнень в МР залежатиме від швидкій адаптації існуючих СВВ до нових загроз. А рівень безпеки мережі буде залежить від вибору стратегії вторгнення в МР.

Висновок

В ході аналізу існуючих загроз при вторгненні в мобільну радіомережу класу MANET були отримані аналітичні вирази для оцінки ймовірності реалізації ризиків порушення нормального функціонування мережі на рівнях моделі OSI.

Визначено, що поширення впливу загроз безпеки інформації окремого вузла на безпеку мобільної радіомережі може викликати появу додаткових загроз безпеки мережі.

З використанням отриманої моделі вторгнень в мобільну радіомережу стало можливим проводити прогнозування та моделювання наслідків вторгнення.

Але з метою розширення можливостей існуючих методів виявлення вторгнень щодо виявлення нових видів вторгнень, прогнозування вторгнень в мобільну радіомережу та забезпечення роботи система виявлення вторгнень в режимі реального часу, розробка даної моделі показала необхідність застосування в системі виявлення вторгнень методів проведення (збору даних, аудиту, аналізу) параметрів рідіосередовища, на що і буде направлена **подальша робота**.

Список літератури

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

2. 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.

3. 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. – К.: НУОУ, 2015. – № 1(22). – С. 103-112.

4. Сальник С.В. 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.

5. 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.

6. Корнеев И.К. Защита информации в офисе / И.К. Корнеев, Е.А. Степанов. – М.: Проспект, 2009. – 51 с.

7. Вихорев С. Как определить источники угроз / С. Вихорев, Р. Кобцев // Открытые системы. – 2002. – № 07-08. – С. 56.

8. Владимиров А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / А.А. Владимиров. – М.: НТ Пресс, 2005. – 463 с.

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

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

11. Чевардін В.Є. Аналіз загроз безпеки інформації в мережах MANET / В.Є. Чевардін, А.В. Романюк, І.М. Діянчук // Збірник наукових праць № 1. – К.: ВІТІ НТУУ "КПІ", 2012. – С. 125 – 134.

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

13. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – СПб: БХВ-Петербург, 2003. – 608 с.

14. Вагизов Ф.Г. Исследование статистического характера распада радиоактивных ядер, распределение Пуассона. Учебно-методическое пособие / Ф.Г. Вагизов, Е.Н. Дулов. – Казань: Казанский (Приволжский) федеральный университет, 2013. – 32 с.

Надійшла до редколегії 1.12.2015

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

МОДЕЛЬ ВТОРЖЕНИЙ В МОБИЛЬНЫЕ РАДИОСЕТИ КЛАССА MANET

С.В.Сальник, В.В. Сальник, О.Я. Сова, Я.А. Стемпковская

В статье представлена модель вторжений в мобильные радиосети класса MANET. Разработка модели базировалась на множестве уязвимостей мобильной радиосети, на которые можно влиять с помощью атак. Было рассмотрено перечень угроз безопасности мобильной радиосети, виды применяемых атак на уровнях сетевой модели OSI, примеры реализации атак и варианты воздействия на сеть, что дало представление о возможностях противника при воздействии на мобильную радиосеть. На основе указанного были получены аналитические выражения для оценки вероятности реализации рисков и вероятностей нарушения безопасности мобильной радиосети на уровнях сетевой модели OSI. Использование полученной модели угроз дает возможность для проведения прогнозирования вторжений противника и моделирования последствий вторжения в режиме реального времени.

Ключевые слова: *мобильные радиосети, MANET, вторжение в мобильную радиосеть.*

A MODEL OF INTRUSION IN MOBILE RADIO NETWORKS CLASS MANET

S.V. Salnyk, V.V. Salnyk, O.Y. Sova, Y.O. Stempkovska

In article presented model of intrusion in mobile radio networks class MANET. Development of model was based on great number of vulnerabilities mobile radio network, on that it maybe to influence by means attacks. The list threats was considered to safety mobile radio network, types of applied attacks on the levels of network model OSI, examples of realization attacks and variants of influence on a network, that gave an idea about possibilities of opponent at influence on a mobile radio network. On the basis of indicated analytical expressions were got for estimation probability of realization risks and probabilities of security mobile radio network breach on the levels network model OSI. The use got model of threats gives an opportunity for realization prognostication encroachments opponent and design consequences of intrusion in real-time mode.

Keywords: *mobile radio networks, MANET, intrusion in mobile radio network.*