**УДК 004.9:517.978.2**

**Грищук Р.В.**

*Житомирський військовий інститут ім. С.П. Корольова*
*Національного авіаційного університету*

# ДИФЕРЕНЦІАЛЬНО – ТЕЙЛОРІВСЬКА МОДЕЛЬ ПЕРЕБУВАННЯ ТЕХНІЧНОГО ОБ'ЄКТА ПІД ВПЛИВОМ МЕТОДІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Стрімкий розвиток інформаційних та комунікаційних технологій становить актуальну проблему для інформаційної безпеки держави [1]. Відсутність в Україні єдиної методології дослідження динаміки зміни перебування технічних об'єктів під впливом методів несанкціонованого доступу (НСД), у залежності від тривалості інформаційних атак на об'єкти, є передумовою подальшого загострення питання інформаційної безпеки, яке є найбільш чутливим для системи національної безпеки та визначальним для забезпечення національного суверенітету [2, 3].

Аналіз останніх іноземних [4-8] та вітчизняних [9-15] нормативних документів, публікацій та досліджень за визначною тематикою показав різнорідність моделей дослідження перебування технічних об'єктів під впливом методів НСД. Відомі якісні моделі носять суб'єктивний характер [4-8]. Результативність застосування якісних моделей визначається рівнем знань, досвіду і інтуїції експерта (менеджера) з безпеки [11]. Сучасні кількісні підходи [12-15] носять по суті статичний характер, оскільки засновані на моментному відображенні стану технічних об'єктів, зафіксованому в дискрети часу, які вже сплинули. Часовий фактор, який має важливе прикладне значення, наприклад для прогнозування стану технічного об'єкта на заданий момент часу при перебуванні його під впливом НСД, у таких моделях не враховується [16]. Таким чином, кількісні моделі потребують доопрацювання, пов'язаного динамічним характером протікання процесу інформаційного конфлікту [17].

Врахування у кількісних моделях фактору часу дозволить відобразити динаміку протікання процесу інформаційного конфлікту у вигляді тенденції його розвитку.

Метою даної роботи є розробка диференціально-тейлорівської моделі перебування технічного об'єкта під впливом методів НСД з можливістю подальших її аналітичних досліджень.

Викладення основного матеріалу.

*Формалізація задачі.* Нехай ймовірності перебування технічного об'єкта під впливом методів НСД $P(t)_{НСД}$ та методів захисту інформації (МЗІ) $P(t)_{МЗІ}$ у складній динамічній системі [18] являють собою повну групу подій:

$$P(t)_{НСД} + P(t)_{МЗІ} = 1. \qquad (1)$$

За початкових умов $P(t=0)_{НСД} = 1$, $P(t=0)_{МЗІ} = 0$ динаміка переходу технічного об'єкта зі стану нападу в стан захищеності та навпаки, описується системою диференціальних рівнянь Колмогорова-Чепмена [17]:

$$\begin{cases} \dfrac{dP(t)_{НСД}}{dt} = -\lambda P(t)_{НСД} + \mu P(t)_{МЗІ}; \\ \dfrac{dP(t)_{МЗІ}}{dt} = \lambda P(t)_{НСД} - \mu P(t)_{МЗІ}, \end{cases} \qquad (2)$$

де $\lambda$ – інтенсивність потоку захисних дій; $\mu$ – інтенсивність потоку інформаційних атак; $t$ – поточний (дискретний) час перебування технічного об'єкта у інформаційному конфлікті.

Протягом тривалості інтервалу здійснення інформаційних атак (спроб НСД) на технічний об'єкт

$$t \in [0, T], \tag{3}$$

де $T$ - тривалість інтервалу, відомими вважаються обмеження на ресурси захисних дій

$$0 < \lambda \le \lambda_{\max} \tag{4}$$

та інформаційних атак

$$0 < \mu \le \mu_{\max}, \tag{5}$$

де $\lambda_{\max}$ – максимальна інтенсивність потоку захисних дій; $\mu_{\max}$ – максимальна інтенсивність потоку інформаційних атак.

*Постановка задачі.* Передбачається, що технічний об'єкт підпадає під вплив максимальних ресурсів суб'єктів інформаційного конфлікту (2) (методів МЗІ та НСД) $\lambda_{\max}$ та $\mu_{\max}$ в границях визначених обмежень (4) та (5) відповідно.

З урахуванням $\lambda_{\max}$ та $\mu_{\max}$ і умов нормування (1) подамо модель інформаційного конфлікту (2) диференціальною моделлю виду

$$\frac{dP(t)_{НСД}}{dt} = \mu_{\max} - (\lambda_{\max} + \mu_{\max}) P(t)_{НСД}. \tag{6}$$

Задача знаходження вигляду моделі перебування технічного об'єкта під впливом методів НСД під час інформаційного конфлікту (2), яка описується динамікою (6), має на меті знаходження аналітичної залежності $P(t)_{НСД}$, від $P(t=0)_{НСД}$, $t$, $\lambda_{\max}$, $\mu_{\max}$ та $T$ і, в загальному вигляді, може бути формалізована функціоналом виду

$$P(t)_{НСД} = f\left(P(t=0)_{НСД}, t, \lambda_{\max}, \mu_{\max}, T\right). \tag{7}$$

Поставлена задача має диференціально-ігровий базис та безкоаліційний характер [19-21].

Основна задача диференціальної гри зводиться до визначення ціни гри, що є критерієм оптимізації, який виражається через оптимальні стратегії (правила поведінки) $\lambda^{ОПТ}$ і $\mu^{ОПТ}$ розподілу наявних ресурсів гравців (суб'єктів інформаційного конфлікту (2)) (4) та (5) та знаходженні траєкторії гри (партії), яка відповідає оптимальним стратегіям [19].

Плата $I$ для широкого класу диференціальних ігор задається у вигляді суми інтегральної та термінальної складових [19-21]. Виходячи з потреби відображення динаміки протікання процесу інформаційного конфлікту (6), плата $I$ повинна мати інтегральний вид, де інтегрування проводитиметься вздовж траєкторії від $t=0$ моменту початку гри до $t=T$ моменту її закінчення (3).

Опишемо інтегральну плату $I$ функціоналом

$$I = \frac{1}{T}\int_0^T P(t)_{НСД}\, dt. \tag{8}$$

З метою пошуку оптимальних правил поведінки у безкоаліційних диференціальних іграх гравці можуть використовувати різні види стратегій - гарантуючі, рівноважні по Нешу і стратегії, які слідують з концепції "погроз і контрпогроз" [19]. Вибір стратегії поведінки гравця у окремо взятій диференціальній грі визначається цілями гри.

У диференціальній грі (3)-(7) цілі суб'єктів інформаційного конфлікту (2) є протилежними. У такому разі, як принцип вибору стратегій, обрано принцип мінімаксу. Згідно даного принципу перший гравець формує стратегію $\lambda$, що мінімізує плату $I$ при умові максимізації плати іншим гравцем

$$I^*(\lambda, \mu) = \min_{\lambda \in E_\lambda} \max_{\mu \in E\mu} I, \tag{9}$$

де $I^*(\lambda, \mu)$ - плата, що відповідає гарантованій стратегії поведінки гравців; $E_\lambda$, $E_\mu$ - замкнені обмежені у евклідових просторах $R_\lambda$ і $R_\mu$ множини, що визначають можливі стратегії гравців.

Другий гравець формує стратегію $\mu$, що максимізує плату $I^*(\lambda, \mu)$ при умові мінімізації плати першим гравцем

$$I^*(\lambda, \mu) = \max_{\mu \in E\mu} \min_{\lambda \in E_\lambda} I. \tag{10}$$

Стратегії $\lambda^{ОПТ}$ і $\mu^{ОПТ}$ розподілу наявних ресурсів (4) та (5) називаються оптимальними, якщо виконується наступне співвідношення

$$I^*\left(\lambda^{ОПТ}, \mu^{ОПТ}\right) = \min_{\lambda \in E_\lambda} \max_{\mu \in E\mu} I = \max_{\mu \in E\mu} \min_{\lambda \in E_\lambda} I. \tag{11}$$

Виконання умови (11) свідчить про наявність сідлової точки гри, яка володіє тією властивістю, що будь-яке відхилення від оптимальної стратегії одним гравцем призводить до втрат в платі при умові вибору оптимальної стратегії іншим гравцем

$$I^*\left(\lambda, \mu^{ОПТ}\right) \geq \min_{\lambda \in E_\lambda} I\left(\lambda, \mu^{ОПТ}\right), \tag{12}$$

$$I^*\left(\lambda^{ОПТ}, \mu\right) \leq \max_{\mu \in E\mu} I\left(\lambda^{ОПТ}, \mu\right). \tag{13}$$

Плата $I^*\left(\lambda^{ОПТ}, \mu^{ОПТ}\right)$, яка відповідає оптимальним стратегіям $\lambda^{ОПТ}$ і $\mu^{ОПТ}$, називається ціною гри.

З урахуванням (8) ціна гри $I^*\left(\lambda^{ОПТ}, \mu^{ОПТ}\right)$, виражена виразом (11), набуватиме виду

$$I^*\left(\lambda^{ОПТ}, \mu^{ОПТ}\right) = \min_{\lambda \in E_\lambda} \max_{\mu \in E\mu} \left(\frac{1}{T} \int_0^T P(t)_{НСД}\, dt\right). \tag{14}$$

*Розв'язання задачі.* Для подальших аналітичних досліджень поведінки моделі (6) застосуємо метод диференціальних перетворень академіка Г.Є. Пухова [22].

Диференціальні перетворення - новий операційний метод, який на відміну від відомих інтегральних перетворень Лапласа і Фур'є, заснований на переводі оригіналів у область зображень за допомогою операції диференціювання [22]. При математичному моделюванні процесу нападу на інформацію, що описується диференціальним рівнянням (6), диференціальні перетворення дозволяють замінити операції диференціювання еквівалентними алгебраїчними операціями як в чисельному, так і в аналітичному вигляді [22].

Диференціально-тейлорівськими перетвореннями (ДТ-перетвореннями) називаються функціональні перетворення виду [22]

$$X(k)=\underline{x}(k)=\frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \quad \underline{\bullet} \quad x(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \tag{15}$$

де $x(t)$ - оригінал, що являє собою безперервну, що диференціюється нескінченне число разів і обмежену разом із всіма своїми похідними, функцію дійсного аргументу $t$; $X(k)$ і $\underline{x}(k)$ рівноцінні позначення диференціального зображення оригіналу, що представляє дискретну (гратчасту) функцію цілочисельного аргументу $k=0,1,2,...$; $H$ - масштабна стала, яка має розмірність аргументу $t$ і часто обирається рівною відрізку $0 \le t \le H$, на якому розглядається функція $x(t)$; $\underline{\bullet}$ - символ відповідності між оригіналом $x(t)$ і його диференціальним зображенням $X(k)=\underline{x}(k)$.

У перетвореннях (15) зліва від символу $\underline{\bullet}$ стоїть пряме перетворення, що дозволяє за оригіналом $x(t)$ знайти зображення $X(k)$, а праворуч – зворотне перетворення, що дозволяє за зображенням $X(k)$ отримати оригінал $x(t)$ у формі степеневого ряду, який є ні чим іншим, як інакше записаним рядом Тейлора з центром у точці $t=0$. Диференціальні зображення $X(k)$ називаються диференціальними Т-спектрами, а значення Т-функції $X(k)$, при конкретних значеннях аргументу $k$, називаються дискретами.

Застосувавши до моделі (6) ДТ-перетворення (15) подамо окремо її доданки.

Згідно рекурентної формули [22] Т-похідна від $\frac{dP(t)_{НСД}}{dt}$ визначається як

$$\frac{dP(t)_{НСД}}{dt} \quad \underline{\bullet} \quad D\,P(k)=\frac{k+1}{H}P(k+1), \tag{16}$$

де $D$ - символ Т-диференціювання.

Зображення сталої $\mu_{\max}$ у моделі (6) набуває виду [23]

$$\mu_{\max} \quad \underline{\bullet} \quad \mu_{\max}\,ъ(k), \tag{17}$$

де $ъ(k)$ - теда [22], $ъ(k)=\begin{cases}1, & k=0;\\ 0, & k\ge 1.\end{cases}$

Операція добутку $P(t)_{НСД}$ на сталу $(\lambda_{\max}+\mu_{\max})$ в моделі (6) визначатиметься рекурентною формулою [22]

$$(\lambda_{\max}+\mu_{\max})P(t)_{НСД} \quad \underline{\bullet} \quad (\lambda_{\max}+\mu_{\max})P(k)_{НСД}\ . \tag{18}$$

Урахування виразів (16), (17) та (18) дозволяє представити вихідну модель диференціальної гри (6) ДТ-моделлю виду

$$\frac{k+1}{H}P(k+1)=\mu_{\max}\,ъ(k)-(\lambda_{\max}+\mu_{\max})P(k)_{НСД}\,. \qquad (19)$$

Приймемо значення масштабної сталої $H$ в ДТ-моделі (19) рівним тривалості інтервалу інформаційних атак $T$ (3), тобто

$$H=T \qquad (20)$$

і згрупуємо доданки в моделі відносно $P(k+1)$. З урахуванням (20) і процедури групування доданків вихідна ДТ-модель (19) матиме кінцевий вид

$$P(k+1)=\frac{T}{k+1}\left(\mu_{\max}\,ъ(k)-(\lambda_{\max}+\mu_{\max})P(k)_{НСД}\right). \qquad (21)$$

Знайдемо дискрети ДТ-моделі (21).

Нульова дискрета $P(0)$ дорівнює початковому значенню оригінала, тобто

$$P(0)=\left[P(t)_{НСД}\right]_{t=0}=1\,. \qquad (22)$$

Решта дискрет ДТ-моделі (21) при значеннях цілочисельного аргументу $k=:1,2,3$ визначається як

$$P(1)=-\lambda_{\max}T\,, \qquad (23)$$

$$P(2)=\frac{1}{2}\lambda_{\max}(\lambda_{\max}+\mu_{\max})T^2\,, \qquad (24)$$

$$P(3)=-\frac{1}{6}\lambda_{\max}(\lambda_{\max}+\mu_{\max})^2T^3\,. \qquad (25)$$

З урахуванням дискрет (22)-(25), диференціальний спектр ДТ-моделі (21) матиме вид відрізку ряду Тейлора

$$1-\lambda_{\max}T+\frac{1}{2}\lambda_{\max}(\lambda_{\max}+\mu_{\max})T^2-\frac{1}{6}\lambda_{\max}(\lambda_{\max}+\mu_{\max})^2T^3\,. \qquad (26)$$

Згідно рекурентної формули [23] ДТ-зображення $I^*$ ціни гри $I^*\left(\lambda^{ОПТ},\ \mu^{ОПТ}\right)$ (14) визначатиметься виразом виду

$$I^*=\sum_{k=0}^{k=\infty}\frac{P(k)_{НСД}}{k+1}\,. \qquad (27)$$

Підстановка у ДТ-зображення ціни гри $I^*$ (27) значень дискрет (22)-(25) ДТ-моделі (21), при значеннях цілочисельного аргументу $k=:1,2,3$, надає їй вид функціонала $I^*\left(\lambda_{\max},\ \mu_{\max}\right)$, тобто

$$I^*\left(\lambda_{\max},\ \mu_{\max}\right)=1-\frac{1}{2}\lambda_{\max}T+\frac{1}{6}\lambda_{\max}\left(\lambda_{\max}+\mu_{\max}\right)T^2-\frac{1}{24}\lambda_{\max}\left(\lambda_{\max}+\mu_{\max}\right)^2T^3. \quad (28)$$

Для знаходження оптимальних стратегій $\lambda^{ОПТ}$ і $\mu^{ОПТ}$ розподілу наявних ресурсів (4) та (5) дослідимо на екстремум функціонал $I^*\left(\lambda_{\max},\ \mu_{\max}\right)$ (28).

Необхідні умови існування екстремуму функціонала $I^*\left(\lambda_{\max},\ \mu_{\max}\right)$ (28) мають вид

$$\begin{cases}\dfrac{\partial I^*\left(\lambda_{\max},\ \mu_{\max}\right)}{\partial\lambda_{\max}}=0;\\[2ex]\dfrac{\partial I^*\left(\lambda_{\max},\ \mu_{\max}\right)}{\partial\mu_{\max}}=0.\end{cases} \quad (29)$$

Знаходження частинних похідних за кожним з рівнянь системи (29) звелося до рішення системи лінійних алгебраїчних рівнянь виду

$$\begin{cases}-\dfrac{1}{2}+\dfrac{1}{3}\lambda_{\max}T+\dfrac{1}{6}\mu_{\max}T=0;\\[2ex]2-\lambda_{\max}T-\mu_{\max}T=0.\end{cases} \quad (30)$$

Розв'язком системи лінійних алгебраїчних рівнянь (30) є стратегії гравців $\lambda_{\max}$ і $\mu_{\max}$, що дорівнюватимуть

$$\lambda_{\max}=\frac{1}{T}, \quad (31)$$

$$\mu_{\max}=\frac{1}{T}. \quad (32)$$

Достатніми умовами існування екстремуму функціонала $I^*\left(\lambda_{\max},\ \mu_{\max}\right)$ (28) є

$$\begin{cases}\dfrac{\partial^2 I^*\left(\lambda_{\max},\ \mu_{\max}\right)}{\partial\lambda_{\max}^2}>0;\\[2ex]\dfrac{\partial^2 I^*\left(\lambda_{\max},\ \mu_{\max}\right)}{\partial\mu_{\max}^2}<0.\end{cases} \quad (33)$$

Оскільки

$$\begin{cases} \dfrac{\partial^2 I^*\left(\lambda_{\max},\ \mu_{\max}\right)}{\partial \lambda_{\max}^2} = \dfrac{1}{3}; \\ \dfrac{\partial^2 I^*\left(\lambda_{\max},\ \mu_{\max}\right)}{\partial \mu_{\max}^2} = -\dfrac{1}{12}\lambda_{\max}, \end{cases} \tag{34}$$

то достатня умова (33) існування екстремуму функціонала (28) виконується.

Виконання необхідних (29) і достатніх (33) умов дозволяє стверджувати, що набір стратегій гравців (31) і (32) є оптимальним

$$\lambda^{ОПТ} = \lambda_{\max}, \tag{35}$$

$$\mu^{ОПТ} = \mu_{\max}, \tag{36}$$

що свідчить про існування сідлової точки гри (11). У результаті відхилення від оптимальної стратегії розподілення ресурсів одним з гравців неминуче призведе до його програшу і відповідно виграшу іншим гравцем.

З урахуванням (35) і (36) ціна гри, виражена функціоналом виду (28), дорівнює

$$I^*\left(\lambda^{ОПТ},\ \mu^{ОПТ}\right) = \frac{2}{3}. \tag{37}$$

Траєкторію диференціальної гри $P(t)_{НСД}$ представлену в загальному виді функціоналом (7), яка відповідає оптимальним стратегіям (35) і (36), отримаємо в аналітичному виді. Для цього застосуємо операцію зворотного перетворення (15) у область оригіналів до ДТ-моделі (21) за її дискретами (22)-(25) та набором оптимальних стратегій (35) і (36)

$$P(t)_{НСД} = 1 - \frac{t}{T} + \left(\frac{t}{T}\right)^2 - \frac{2}{3}\left(\frac{t}{T}\right)^3. \tag{38}$$

Траєкторія (38), отримана на основі ДТ-моделі (21), відображає динаміку перебування технічного об'єкта під впливом методів несанкціонованого доступу у заданий момент часу $t$ на визначеному часовому інтервалі (3).

Таким чином диференціальна гра (2)-(7) вирішена повністю. Знайдено ціну гри (37), оптимальні стратегії розподілу ресурсів (35), (36) і траєкторію гри (38), яка відповідає оптимальним стратегіям.

Висновки та перспективи подальших досліджень. Розроблена ДТ-модель перебування технічного об'єкта під впливом методів несанкціонованого доступу (21) дозволяє природнім шляхом відображати динаміку (часовий фактор) протікання інформаційного конфлікту (2). Розроблена ДТ-модель (21) дозволяє оцінювати поточний стан перебування технічного об'єкта у будь-який момент часу на заданому часовому інтервалі здійснення інформаційних атак (3) та є адекватною моделлю реальним процесам нападу на інформацію. ДТ-модель (21) забезпечує природне поєднання дискретної $t$ та неперервної $\tau$ інформації. Розроблена ДТ-модель дозволяє визначати стан перебування технічного об'єкта під впливом методів НСД для моментів часу у минулому, теперішньому і порівняно недалекому майбутньому.

У подальшому планується провести дослідження поведінки моделі (21) при відхиленнях поведінки гравців від оптимальних стратегій (35) і (36).

### *Список літератури*

1. *Хорошко В.А.* Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатов. – К.: Юниор, 2003. – 478 с.

2. *Даник Ю.Г.* Національна безпека: запобігання критичним ситуаціям: Монографія / Даник Ю.Г., Катков Ю.І., Пічугін М.Ф. – Житомир: Рута, 2006. – 388 с.

3. *Про основи національної безпеки України*: Закон України № 964 - IV від 19.06.03.

4. *ISO 15408.* The Common Criteria for Information Technology Security Evaluation.

5. *Information* Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-the Netherlands-the United Kingdom. – Department of Trade and Industry, London, 1991.

6. *Canadian* Trusted Computer Product Evaluation Criteria, Version 3.0. – Canadian System Security Center, Communications Security Establishment, Government of Canada, 1993.

7. *Department* of Defense Trusted Computer System Evaluation Criteria, DoD5200.28-STD, 1983.

8. *Руководящий* документ. Средства вычислительной техники. Межсетевые экраны. Защита от НСД. Показатели защищённости от НСД к информации. – М.: Гостехкомиссия РФ, 1996.

9. *ДСТУ 3396.0-96.* Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.

10. *НД ТЗІ 2.2-001-98.* Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України. - введ. 1998.

11. *Поповский В.В.* Защита информации в телекоммуникационных системах: Учебник. Том 1 / Поповский В.В., Персиков А.В. – Харьков: ООО "Компания СМИТ", 2006 – 238 с.

12. *Браіловський М.М.* Кількісно-якісна оцінка рівня інформаційної безпеки / Браіловський М.М., Габович А.Г., Горобець А.Ю., [та ін.] // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2006. - № 9 (103), Частина 1. – с. 14-17.

13. *Андреев В.И.* Количественная оценка защищённости технических объектов с учётом их функционирования / Андреев В.И., Козлов В.С., Хорошко В.А. // Захист інформації. – К.: НАУ, 2004. - № 2. – С. 47-50.

14. *Козлов В.С.* Количественная оценка защищённости информации / Козлов В.С., Хорошко В.А. // Захист інформації. – К.: НАУ, 2003. – № 4. – С. 67-73.

15. *Козлова К.В.* Кількісна оцінка захисту радіоелектронних об'єктів (РЕО) / Козлова К.В., Хорошко В.О. // Захист інформації. – К.: ДІТС, 2007. - № 1. С. 30-32.

16. *Азаренко Е.В.* Проектирование автоматизированных систем управления на компьютерных сетях: Монография / Азаренко Е.В., Герасимов Б.М., Шохин Б.П. – Севастополь: Гос. Океанариум, 2007. – 272 с.

17. *Ігнатов В.О.* Динаміка інформаційних конфліктів в інтелектуальних системах / Ігнатов В.О., Гузій М.М. // Проблеми інформатизації та управління. – К.: НАУ, 2005. – Вип. 15. – С. 88-92.

18. *Р- моделювання* складних динамічних систем / [Г.Л. Баранов, М.М. Браіловський, А.А. Засядьмо та ін.]; за ред. проф. Г.Л. Баранова та проф. В.О. Хорошко. – К.: ДУІКТ, 2008 – 132 с.

19. *Васильев В.В.* Моделирование задач оптимизации и дифференциальных игр / В.В. Васильев, В.Л. Баранов. – К.: Наукова думка, 1989. – 286 с.

20. *Вайсборд Э.М.* Введение в дифференциальные игры нескольких лиц и их приложения / Э.М. Вайсборд, В.И. Жуковский. – М.: Советское радио, 1980. – 304 с.

21. *Теорія* графів у задачах розподілу ресурсів. Кн. 2. Диференціально-ігровий підхід до моделювання систем [підруч. для студ. техн. спец. вищ. навч. закл.] / Лістровий С.В., Луханін М.І., Мартинова О.П., Семчук Р.В. – Харків: ПП Видавництво "Нове слово", 2007. – 144 с.

22. *Пухов Г.Э.* Дифференциальные спектры и их модели. – К.: Наук. думка, 1990. – 184 с.

23. *Диференціальні* перетворення для комп'ютерного моделювання керуючих систем: [навч. посібн. для студ. вищ. навч. закл.] / О.І. Стасюк, В.Л. Баранов, Г.Л. Баранов, О.Г. Фролова. – К.: КУЕТТ, 2005. – 135 с.

**УДК 681.3**

**Дудикевич В.Б., Піскозуб А.З., Тимошик Н.П., Тимошик Р.П., Дуткевич Т.В.**
*Национальный университет "Львівська політехніка"*

## МЕТОДИ ТА ЗАСОБИ АНАЛІЗУ СИСТЕМИ-ПРИМАНКИ В ПРОЦЕСІ ЗЛАМУ

Підхід до отримання сигнатур від систем приманок залежить від знань про методи компрометації робочих систем та процедур аналізу інцидентів, які включають в себе порівняння еталонної операційної системи (ОС) з її скомпрометованою версією. Для цього нам необхідно розглянути можливі методики зламу чи компрометації систем та у відповідності до них сформувати власну процедуру для розслідування інцидентів в системах-приманках, процесів та причин успішного проникнення, а також можливостей моніторингу критичних областей, завдяки яким проникнення може мати успіх.

Ідея використання системи приманок дуже зручна для аналітиків безпеки завдяки наступній особливості: в спеціально підготовлену, привабливу для зловмисника систему (наприклад, система може містити якусь відому або невідому досі вразливість) потрапляє кваліфікований зловмисник. Завдяки спеціалізованому програмному забезпеченню існує можливість стеження за діями зловмисника на приманці та отримання інформації про найновіші методи, засоби та підходи в реалізації атак та шкідливого впливу (malware) на комп'ютерні системи та мережі [1].

Метою даної статті є систематизація методів та засобів аналізу систем-приманок в процесі зламу комп'ютерних систем чи мереж та рекомендації щодо організації розслідування зламу, вибору засобів збору та аналізу подій.

Таким чином, завдяки правильному розгортанню та конфігурації системи-приманки таке проникнення може бути проаналізоване і відповідно може бути створене відповідне правило, за допомогою якого система виявлення атак зможе зупинити подібну атаку на важливу робочу систему чи мережу [2]. Для цього рекомендується використовувати спеціалізовані приманки, тобто розділяти системи-приманки на складові компоненти, наприклад: приманка з надійно захищеною ОС, але вразливим сервісом ( для прикладу приманка лише з незахищеним веб-сервером чи приманка з вразливою СУБД); приманка з оновленою та захищеною ОС [3]. Для зручності аналізу атак та даних, які необхідно аналізувати, атаки на прикладні сервіси можна розбити на такі класи як атаки на сервіси та атаки на операційні системи.

Атаками на сервіси можна вважати:

- атаки відмови в обслуговуванні сервісу (DoS, DDoS);
- атаки з використанням вразливості сервісу (веб, dns, поштовий сервіс) з метою отримання принаймні мінімального локального доступу до системи або читання конфігурації системи (файлів паролів, конфігурації системи, параметрів фаєрволів);
- атаки з використанням неправильного конфігурування сервісу (firewall, privilegies overflow, php-injection, не встановлені chroot обмеження, списки контролю доступу (ACL), SELinux);
- атаки на бази даних з метою викрадення або зміни інформації (зміна вмісту веб-сторінки, перенаправлення на підставні ресурси та викрадення конфіденційної інформації, SQL Injection).

Друга категорія атак – атаки на операційні системи, є доволі поширена і причинами її успішності є:

- неправильна реалізація мережевої взаємодії, контролю трафіку та мережного стеку;