УДК 004.9:517.978.2

ДИФЕРЕНЦІАЛЬНО-ІГРОВА МОДЕЛЬ ШАБЛОНУ НОРМАЛЬНОЇ ПОВЕДІНКИ WEB–СЕРВЕРУ

Р.В. Грищук
Житомирський військовий інститут імені С. П. Корольова Національного авіаційного університету

Вперше розроблено диференціально-ігрову модель шаблону нормальної поведінки Web-сервера. Модель дозволяє врахувати динаміку розвитку процесу атак на Web-сервер та гарантовано управляти рівнем його захищеності.

In this article differential-game model of the web server normal behavior template is developed for the first time. Developed model allows to take into account the dynamics of the attack progress on web server, that permits to discover the possibilities of guaranteed control of its level protection.

Впервые разработана дифференциально-игровая модель шаблона нормального поведения Web-сервера. Разработанная модель позволяет учитывать динамику развития атаки на Web-сервер, при этом открываются возможности гарантированного управления уровнем его защищённости.

Вступ

Відомо [1, 2], що віддалений мережний доступ потенційних користувачів до інформаційних ресурсів у мережі Internet здійснюється за протоколом http (Hyper Text Transfer Protocol), який ініціює запит шляхом встановлення протоколу TCP (Transmission Control Protocol) з'єднання з визначеним портом, як правило, вісімдесятим. Технологічні аспекти з організації такого доступу покладаються на Web-сервери. Стрімке зростання за останній рік динаміки атак на Web-сервери державних установ та урядових організацій, провідних фінансових структур та підприємств в світі та в Україні, зокрема [1-4], призводить до зниження якості функціонування серверних технологій, чим значно активізує проблему захисту інформації на об'єктах критичної інфраструктури. У рамках визначеної проблеми задача підвищення рівня захищеності Web-серверів набуває особливої актуальності.

І. Аналіз останніх досліджень і публікацій

З аналізу доступних джерел [5-11] з'ясовано, що одним із перспективних шляхів підвищення рівня захищеності Web-серверів є вдосконалення активних засобів захисту інформації на базі систем виявлення атак (вторгнень) (СВА) – IDS (Intrusion Detection Systems) [5-9]. На сьогоднішній день таких систем відомо близько сотні [1, 5-10]. Аналіз концептуальних основ побудови найбільш поширених комерційних СВА на базі хосту – Intruder Alert (компанія Symantec), на базі мережі – Cisco Secure Scanner (компанія Cisco Systems), гібридної СВА – RealSecure (компанія Internet Security Systems) та некомерційних СВА ASAX (University of Namur, Belgium), SHADOW

(Naval Surface Warfare Center, Dahlgren Division) та NetSTAT (University of California at Santa Barbara), відповідно, дозволяє зробити висновок, що робота кожної із систем ґрунтується на методах визначення аномалій та визначення зловживань. Базисом зазначених методів є моделі шаблонів (профілів) поведінки. Приведемо детальний аналіз методів першої групи.

Методи визначення аномалій призначені для виявлення невідомих атак і вторгнень на Web-сервери на основі моделей шаблонів нормальної поведінки (ШНП) [5-11]. Для побудови моделей ШНП використовуються методи статистичного виявлення, нейронних мереж, теорії масового обслуговування тощо. Характерним недоліком моделей ШНП на базі методів статичного виявлення є велика кількість помилкових спрацювань системи, яка обумовлена помилками першого (пропуск атаки – false negative) та другого (віднесення ШНП до класу атак – false positive) роду. Недосконалість методики проектування нейромережевих моделей ШНП призводить до потреби їх тривалого навчання за рахунок великої кількості спроб та помилок [11]. Застосування відомих марківських моделей ШНП на базі ланцюгів з послідовною зміною станів не дозволяє виявляти аномалії при отриманні невідомих паттернів. Паттерн – сукупність значень параметрів оцінки системи [9].

Отже, з приведеного критичного аналізу останніх досліджень та публікацій зрозуміло, що задача підвищення рівня захищеності Web-серверів зводиться до розробки нових моделей ШНП, а її розв'язання є нагальною потребою сьогодення. Тому метою статті є розробка диференціально-ігрової моделі шаблону нормальної поведінки Web-серверу.

II. Викладення основного змісту досліджень

Твердження. Під атакою на Web-сервер слід розуміти порушення нормальної працездатності окремого хосту шляхом знищення або модифікації його змісту з подальшим отриманням привілейованого доступу до нього [1, 2, 5]. Одними з найбільш розповсюджених видів атак на Web-сервер фахівцями [3-5] визнано механізми DoS-атак (Denial of Service), які спрямовано на відмову в обслуговуванні. Суть таких атак зводиться до наступного [1-11]:

– на Web-сервер, що атакується, противником посилається некоректний запит, призначений для зациклення процедур обробки, які в кінцевому рахунку призводять до зависання системи;

– перевантаження пропускної здатності комутаційних каналів шляхом генерування трафіка небажаних та непотрібних пакетів або хибних повідомлень про поточний стан мережних ресурсів;

– надходження великої кількості фіктивних запитів від розподілених користувачів або програм на встановлення зв'язку з Web-сервером. Сукупність розподілених користувачів та шкідливого програмного забезпечення називається Boot-мережами, а відповідні атаки – DDoS-атаками (Distributed DoS);

– перевантаження противником (противниками) обчислюваних ресурсів Web-серверу шляхом санкціонованих запитів на використання серверних програмних аплікацій, наприклад таких як PHP, Java, Python тощо.

З аналізу можливих механізмів реалізації DoS- і DDoS-атак на Web-сервер встановлено: DoS- і DDoS-атаки породжують інформаційний конфлікт в інформаційній системі, що передбачає антагоністичну взаємодію двох гравців (суб'єктів конфлікту) – противника та системи. Отже, виходячи з встановленого, сформульована в статті мета може бути досягнута шляхом адаптації основних положень теорії моделювання процесів нападу на інформацію методами теорії диференціальних ігор [14, 15] та диференціальних перетворень [16].

Вихідні дані для моделювання зібрано в період з 01.08.2009 року по 31.01.2010 року для Web-серверу Apache 2.2.10 (Linux|SUSE) з використанням опції Webalizer Logfile Analysis на основі аналізу log-файлів. Мінімальний період спостереження T обрано рівним 24 годинам (рис. 1), середній – календарному місяцю (рис. 2), максимальний – півроку, що адекватно відповідає циклічності звернень користувачів до ресурсу. Збільшення інтервалу спостереження недоцільно з практичної точки зору.

Сервер забезпечував доступ користувачів мережі Internet до інформаційного ресурсу наукової установи за виділеним каналом зі швидкістю передачі даних 15 Мбіт/с у вигляді динамічної Web-сторінки, середній об'єм якої складає 1 Мбайт. Доступ на сервері відкритий для усіх користувачів мережі Internet. Вимоги за доступністю до інформації на сервері – високі. Відмова в обслуговуванні – недопустима. Вимоги за конфіденційністю – низькі. Інформація призначена для широкого кола користувачів. Вимоги за цілісністю – високі, оскільки деструктивний вплив на інформацію призводить до дезорганізації діяльності як підлеглих та взаємодіючих підрозділів, так і порушення нормальної роботи установи в цілому.

Як параметр оцінки захищеності Web-серверу від DDoS-атаки на визначених інтервалах спостереження (рис. 1, 2), обрано об'єм середнього вихідного мережного трафіка за протоколом http.

Рис. 1. Флуктуація середньодобового трафіка:
період спостереження з 01.08.2009 року по 31.01.2010 року

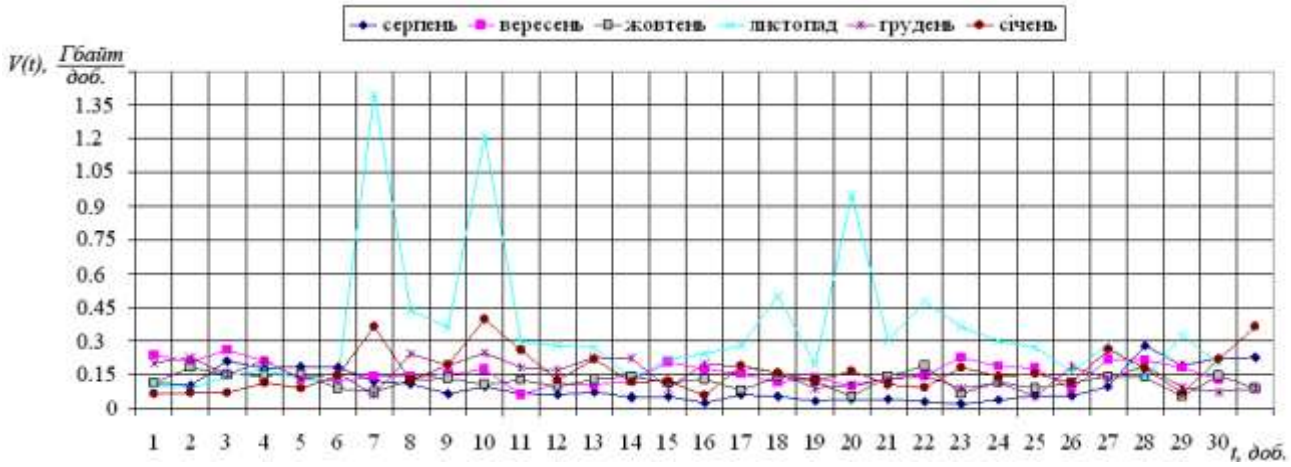

Рис. 2. Флуктуація місячного та піврічного трафіка:
період спостереження з 01.08.2009 року по 31.01.2010 року

Спираючись на експлуатаційну статистику досліджуваного Web-серверу Apache (рис. 1, 2), ШНП подамо графовою моделлю (рис. 3). В моделі (рис. 3) над кружечками, що визначають множину станів $\{P_z(t)\}$, де $z = 0...3$ – стани, в яких може перебувати Web-сервер з відповідними ймовірностями, стрілками визначено всі можливі його переходи зі стану в стан.

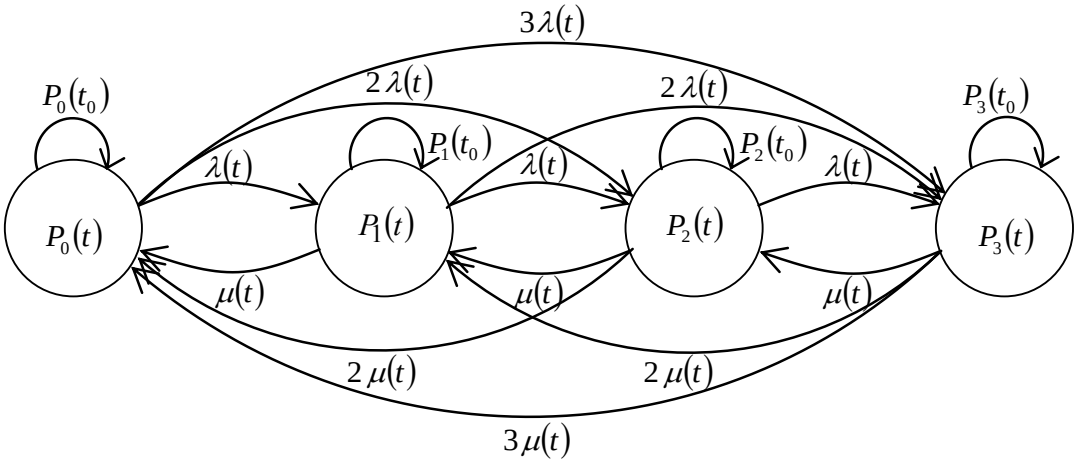

Рис. 3. Графова модель шаблону нормальної поведінки Web-сервера

Над стрілками переходів (рис. 3) проставлено параметри потоків подій $\lambda(t)$ та $\mu(t)$, що переводять сервер зі стану в стан. Під потоками подій $\lambda(t)$ та $\mu(t)$ слід розуміти стратегії гравців, що обираються ними для організації захисних дій та DDoS-атак відповідно. Передбачається, що $P_0(t)$ – ймовірність відмови Web-серверу від обслуговування під впливом DDoS-атаки, $P_1(t)$ – ймовірність перебування Web-серверу під впливом DDoS-атаки при дії методів захисту інформації (МЗІ), $P_2(t)$ – ймовірність перебування Web-серверу під впливом МЗІ при дії DDoS-атаки, $P_3(t)$ – ймовірність перебування Web-серверу під впливом МЗІ. $P_z(t_0)$ – початкові умови при перебуванні серверу в z-му стані; t_0 – початок моделювання.

Особливістю запропонованої графової моделі ШНП (рис. 3) є те, що вона передбачає усі можливі переходи сервера зі стану в стан під впливом відповідних стратегій. Як стверджується в [17], ймовірність переходів, наприклад з нульового у четвертий стани, наближається до нуля, тому в моделі такі переходи не розглядаються. Виходячи з рис. 3 та спираючись на дослідження [14, 15], динаміку інформаційного конфлікту, який протікає під час DDoS-атаки на Web-сервер Apache, подамо в формалізованому вигляді системою нелінійних диференціальних рівнянь Колмогорова-Чепмена

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -6\,\lambda(t)P_0(t) + \mu(t)P_1(t) + 3\,\mu(t)P_3(t); \\ \dfrac{dP_1(t)}{dt} = -(\lambda(t)+\mu(t))P_1(t) + \lambda(t)P_0(t) + \mu(t)P_2(t) + 2\,\mu(t)P_3(t); \\ \dfrac{dP_2(t)}{dt} = -(\lambda(t)+\mu(t))P_2(t) + \lambda(t)P_1(t) + 2\,\lambda(t)P_0(t) + \mu(t)P_3(t); \\ \dfrac{dP_3(t)}{dt} = -6\,\mu(t)P_3(t) + \lambda(t)P_2(t) + 3\,\lambda(t)P_0(t). \end{cases} \quad (1)$$

Нормуюча умова для системи (1), має вигляд

$$\sum_{z=0}^{3} P_z(t) = 1, \quad (2)$$

де початкові умови $P_0(t_0)=1$, $P_1(t_0)=P_2(t_0)=P_3(t_0)=0$.

Нехай стратегії гравців розподілені за лінійними законами загального вигляду

$$\lambda(t) = \lambda t, \quad (3) \qquad \mu(t) = \mu t, \quad (4)$$

де λ та μ – параметри законів розподілу стратегій гравців, які невідомі; t – часовий аргумент, $t \in [t_0, T]$. Ресурси гравців (3) та (4) обмежені:

$$\lambda_{\min}(t) \le \lambda(t) \le \lambda_{\max}(t), \quad (5) \qquad \mu_{\min}(t) \le \mu(t) \le \mu_{\min}(t), \quad (6)$$

де $\lambda_{\min}(t)$ і $\mu_{\min}(t)$ – мінімальні, а $\lambda_{\max}(t)$ і $\mu_{\max}(t)$ – максимальні інтенсивності потоків захисних дій та інформаційних атак відповідно. Стратегії гравців $\lambda(t)$ та $\mu(t)$, що визначають їх ресурси, належать замкненим множинам $\Lambda \in E_\lambda$ та $M \in E_\mu$, які обмежені в евклідових просторах R_λ і R_μ.

Під час інформаційного конфлікту гравці намагаються досягти протилежних цілей. Ціль гравця, що захищається від DDoS-атаки, забезпечити функціональну стійкість Web-серверу шляхом гарантування його захищеності, а гравця, що атакує – досягнути відмови серверу від обслуговування. Для цього гравець, що захищається від DDoS-атаки, намагається отримати найменший програш за рахунок вибору такої власної стратегії $\lambda(t)$, яка мінімізує плату $I_1(t, P_0(t), \lambda(t), \mu(t))$, за умови максимізації плати другим гравцем, тобто

$$\min_{\lambda(t) \in E_\lambda} \max_{\mu(t) \in E_\mu} = I_1(t, P_0(t), \lambda(t), \mu(t)), \quad (7)$$

де $I_1\left(t, P_0(t), \lambda(t), \mu(t)\right) = I_1$ – плата, що є усередненою ймовірністю перебування Web–серверу під впливом DDoS-атаки. Плата визначається як

$$I_1 = \frac{1}{T}\int_{t_0}^{T} P_0(t)\,dt \tag{8}$$

при обмеженнях

$$0 \le I_1 \le I_{1\mathbf{max}}, \text{ де } I_{1\mathbf{max}} = 1. \tag{9}$$

Для досягнення цілі DDoS-атаки противник (другий гравець) намагатиметься отримати найбільший виграш за рахунок вибору такої власної стратегії $\mu(t)$, яка максимізує плату $I_1\left(t, P_0(t), \lambda(t), \mu(t)\right)$, за умови її мінімізації іншим гравцем, тобто

$$\max_{\mu(t)\,\in E_\mu}\ \min_{\lambda(t)\,\in E_\lambda} = I_1\left(t, P_0(t), \lambda(t), \mu(t)\right). \tag{10}$$

Якщо виконується співвідношення рівності критеріїв (6) та (9)

$$\min_{\lambda(t)\,\in E_\lambda}\ \max_{\mu(t)\,\in E_\mu} = I_1\left(t, P_0(t), \lambda(t), \mu(t)\right) = \max_{\mu(t)\,\in E_\mu}\ \min_{\lambda(t)\,\in E_\lambda} = I_1\left(t, P_0(t), \lambda(t), \mu(t)\right) =$$

$$= I_1\left(t, P_0^{HNP\,opt}(t), \lambda^{opt}(t), \mu^{opt}(t)\right) = I_1^{Gar}, \tag{11}$$

то стратегії $\lambda^{opt}(t)$ і $\mu^{opt}(t)$ називаються оптимальними, а $P_0^{HNP\,opt}(t)$ – оптимальна траєкторія, яка підлягає визначенню з системи (1) за критерієм (6) та є диференціально-ігровою моделлю ШНП поведінки Web-серверу для гравця, що атакує; $I_1\left(t, P_0^{HNP\,opt}(t), \lambda^{opt}(t), \mu^{opt}(t)\right)$, I_1^{Gar} – ціна гри, що визначає гарантований рівень захищеності Web-серверу, який досягається за рахунок вибору гравцями оптимальних стратегій $\lambda^{opt}(t)$ та $\mu^{opt}(t)$.

При відхиленні будь-ким з гравців від оптимальної стратегії, неминуче виникають втрати в платі, тобто

$$I_1\left(t, P_0(t), \lambda(t), \mu^{opt}(t)\right) \ge \min_{\lambda(t)\,\in E_\lambda} I_1\left(t, P_0(t), \lambda(t), \mu^{opt}(t)\right). \tag{12}$$

Знаходження вигляду диференціально-ігрової моделі ШНП Web-серверу $P_0^{HNP\,opt}(t)$ здійснимо за загальною методологією [14, 15] з використанням методу Р-перетворень академіка Г. Є. Пухова [15]. З використанням прямого диференціального перетворення [16] система (1) в області Р-зображень матиме вигляд

$$\begin{cases} P_0(k+1) = \dfrac{T}{k+1}\left(-6\ \Lambda(k) * P_0(k) + \mathrm{M}(k) * P_1(k) + 3\,\mathrm{M}(k) * P_3(k)\right); \\ P_1(k+1) = \dfrac{T}{k+1}\left(-(\Lambda(k) + \mathrm{M}(k)) * P_1(k) + \Lambda(k) * P_0(k) + \mathrm{M}(k) * P_2(k) + 2\,\mathrm{M}(k) * P_3(k)\right); \\ P_2(k+1) = \dfrac{T}{k+1}\left(-(\Lambda(k) + \mathrm{M}(k)) * P_2(k) + \Lambda(k) * P_1(k) + 2\ \Lambda(k) * P_0(k) + \mathrm{M}(k) * P_3(k)\right); \\ P_3(k+1) = \dfrac{T}{k+1}\left(-6\,\mathrm{M}(k) * P_3(k) + \Lambda(k) * P_2(k) + 3\ \Lambda(k) * P_0(k)\right), \end{cases} \tag{14}$$

де $\{P_z(k)\}$, $\Lambda(k)$, $\mathrm{M}(k)$ – диференціальні зображення оригіналів $\{P_z(t)\}$, $\lambda(t)$ та $\mu(t)$ відповідно, що представляють собою дискретні функції цілочисельного аргументу $k = 0, 1, 2, \ldots$; $*$ – символ операції множення в області зображень. Система (13) справедлива при рівності масштабної сталої H періоду спостереження T ($H = T$).

З урахуванням властивості T-добутку диференціальних зображень [16] $\Lambda(k) * P_z(k)$ та $\mathrm{M}(k) * P_z(k)$, один з доданків в яких являє собою сталі λ та μ множені на цілу степінь незалежного змінного T^m (при $m = 1$), в загальному вигляді маємо

$$\Lambda(k) * P_z(k) = \lambda T P_z(k-1) = \begin{cases} \lambda T P_z(k-1), & k \geq 1, \\ 0, & k < 1, \end{cases} \tag{15}$$

$$\mathrm{M}(k) * P_z(k) = \mu T P_z(k-1) = \begin{cases} \mu T P_z(k-1), & k \geq 1, \\ 0, & k < 1. \end{cases} \tag{16}$$

Система спектральних рівнянь (14) з урахуванням (15) та (16) матиме вигляд

$$\begin{cases} P_0(k+1) = \dfrac{T^2}{k+1}\left(-6\lambda P_0(k-1) + \mu P_1(k-1) + 3\mu P_3(k-1)\right); \\ P_1(k+1) = \dfrac{T^2}{k+1}\left(-(\lambda+\mu)P_1(k-1) + \lambda P_0(k-1) + \mu P_2(k-1) + 2\mu P_3(k-1)\right); \\ P_2(k+1) = \dfrac{T^2}{k+1}\left(-(\lambda+\mu)P_2(k-1) + \lambda P_1(k-1) + 2\lambda P_0(k-1) + \mu P_3(k-1)\right); \\ P_3(k+1) = \dfrac{T^2}{k+1}\left(-6\mu P_3(k-1) + \lambda P_2(k-1) + 3\lambda P_0(k-1)\right). \end{cases} \tag{17}$$

Присвоюючи послідовно цілочисельні значення аргументу $k = 0, 1, 2, \ldots$, від початкових умов

$$P_0(0) = \left[P_0(t_0)\right] = 1, \; P_1(0) = P_2(0) = P_3(0) = 0, \tag{18}$$

визначаємо дискрети диференціального спектра для диференціально-ігрової моделі ШНП Web-сервера. Дискрети мають вигляд

$$P_0(1) = 0, \tag{19}$$

$$P_0(2) = -3\lambda T^2, \tag{20}$$

$$P_0(3) = 0, \tag{21}$$

$$P_0(4) = \frac{1}{4}\lambda(18\lambda + 7\mu)T^4, \tag{22}$$

$$P_0(5) = 0, \tag{23}$$

$$P_0(6) = -\frac{1}{12}\lambda\left(3\lambda(18\lambda + 7\mu) + \frac{1}{4}\mu(77\lambda + 53\mu)\right)T^6. \tag{24}$$

В області зображень плата (7), після підстановки дискрет (18)-(24), має вигляд

$$I_1 = \sum_{k=0}^{k=\infty} \frac{P_0(k)}{k+1} \approx 1 - \lambda T^2 + \frac{1}{20}\lambda(18\lambda + 7\mu)T^4 - \frac{1}{84}\lambda\left(3\lambda(18\lambda + 7\mu) + \frac{1}{4}\mu(77\lambda + 53\mu)\right)T^6. \tag{25}$$

Дослідження на екстремум фунціонала (25) згідно з виразами

$$\begin{cases} \dfrac{\partial I_1(\lambda,\mu)}{\partial \lambda} = 0; \\ \dfrac{\partial I_1(\lambda,\mu)}{\partial \mu} = 0 \end{cases} \tag{26}$$

зводиться до розв'язання системи лінійних алгебраїчних рівнянь

$$\begin{cases} (36\lambda + 7\mu)T^2 - 20 = 0; \\ \dfrac{7}{5} - \dfrac{1}{42}\left(\dfrac{161}{2}\lambda + 53\mu\right)T^2 = 0. \end{cases} \tag{27}$$

Розв'язання системи (27) дозволяє визначити невідомі параметри λ та μ в стратегіях гравців (2) та (3)

$$\lambda = \frac{6484}{13445T^2} \approx 0.4823\frac{1}{T^2}, \tag{28}$$

$$\mu = \frac{5068}{13445T^2} \approx 0.3769\frac{1}{T^2}. \tag{29}$$

Виконання достатніх умов

$$\begin{cases} \dfrac{\partial^2 I_1(\lambda,\mu)}{\partial \lambda^2} > 0; \\ \dfrac{\partial^2 I_1(\lambda,\mu)}{\partial \mu^2} < 0, \end{cases} \Rightarrow \begin{cases} 36T^2 > 0; \\ -\dfrac{53}{42}T^2 < 0 \end{cases} \tag{30}$$

дозволяє стверджувати, що знайдені параметри (28) та (29) забезпечують максимум та мінімум функціонала (25)

Перевірка умов існування сідлової точки в даній диференціальній грі передбачає знаходження параметра дельта Δ, що визначається аналітичною залежністю [19]

$$\Delta = \left(\frac{\partial^2 I_1(\lambda,\mu)}{\partial\lambda\,\partial\mu}\right)^2 - \left(\frac{\partial^2 I_1(\lambda,\mu)}{\partial\lambda^2}\right)\left(\frac{\partial^2 I_1(\lambda,\mu)}{\partial\mu^2}\right). \tag{31}$$

Оскільки згідно з (31) для умов (30) $\Delta > 0$ ($\Delta = 0.33T^8$, при $T > 0$), то в даній диференціальній грі існує сідлова точка. Отже знайдені коефіцієнти (28) та (29), що визначають вигляд стратегій гравців при переході до області оригіналів з використанням зворотних перетворень [16] є оптимальними

$$\lambda_{\min}^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \Lambda(k) \approx 0{,}4823\frac{t}{T^2}, \tag{32}$$

$$\mu_{\max}^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \mathrm{M}(k) \approx 0{,}3769\frac{t}{T^2}. \tag{33}$$

Гарантований рівень захищеності I_1^{Gar} для досліджуваного Web-серверу Apache від DDoS-атаки на добовому, місячному та піврічному інтервалах спостереження, за визначених початкових умов та після підстановки (28) і (29) в (10), дорівнює

$$I_1^{Gar} \approx 0{,}6672. \tag{34}$$

Диференціально-ігрова модель ШНП Web-серверу, з урахуванням (32) та (33), при переході в область оригіналів має вигляд

$$P_0^{HNP\,opt}(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k\left[P_0(k)\right]_{\substack{\lambda=\lambda^{opt}\\ \mu=\mu^{opt}}}\approx\sum_{k=0}^{k=6}\left(\frac{t}{T}\right)^k\left[P_0(k)\right]_{\substack{\lambda=\lambda^{opt}\\ \mu=\mu^{opt}}}=$$

$$=1-1{,}4469\left(\frac{t}{T}\right)^2+1{,}3649\left(\frac{t}{T}\right)^4-0{,}8747\left(\frac{t}{T}\right)^6. \qquad (35)$$

При відхиленні гравців від оптимальних стратегій (31) та (32) модель ШНП (34) визначатиметься точною аналітичною моделлю

$$P_0(t)=1-3\lambda t^2+\frac{1}{4}\lambda(18\lambda+7\mu)t^4-\frac{1}{12}\lambda\left(3\lambda(18\lambda+7\mu)+\frac{1}{4}\mu(77\lambda+53\mu)\right)t^6. \qquad (36)$$

III. Змістовний аналіз диференціально-ігрової моделі ШНП

З моделі (36) та отриманої оцінки гарантованого рівня захищеності I_1^{Gar} (34) зрозуміло, що досліджуваний Web-сервер Apache при виборі гравцями оптимальних стратегій (32) та (33) з ймовірністю $0{,}6672$ відмовить від обслуговування. В таблиці приведено аналітичні моделі ШНП для різних умов експлуатації Web–серверу та результати моделювання з оцінки його захищеності при виборі гравцями оптимальних стратегій та при їх відхиленні від них. На рис. 4 приведено графіки ШНП для умов, вихідні дані на які наведено у таблиці.

Таблиця. Вихідні дані для моделювання

Модель ШНП $P_0^{HNP\,opt}(t)=1-1.4469\left(\frac{t}{T}\right)^2+1.3649\left(\frac{t}{T}\right)^4-0.8747\left(\frac{t}{T}\right)^6$, для умов $P_0(t_0)=1,\ P_1(t_0)=P_2(t_0)=P_3(t_0)=0$								
Стратегії	$\lambda(t)$	$\lambda^{opt}(t)=0.4823\frac{t}{T^2}$	$0.4823\frac{t}{T^2}$	$0.4823\frac{t}{T^2}$	$0.6029\frac{t}{T^2}$	$0.7235\frac{t}{T^2}$	$0.9646\frac{t}{T^2}$	$0.6029\frac{t}{T^2}$
	$\mu(t)$	$\mu^{opt}(t)=0.3769\frac{t}{T^2}$	$0.2827\frac{t}{T^2}$	$0.1885\frac{t}{T^2}$	$0.3769\frac{t}{T^2}$	$0.3769\frac{t}{T^2}$	$0.3769\frac{t}{T^2}$	$0.1885\frac{t}{T^2}$
Рівень захищеності	I_1	$I_1^{Gar}=0.6658$	0.665	0.6631	0.5837	0.4887	0.2331	0.5869
Модель ШНП $P_0^{HNP\,opt}(t)=0.5-0.4134\left(\frac{t}{T}\right)^2+0.3445\left(\frac{t}{T}\right)^4-0.1792\left(\frac{t}{T}\right)^6$, для умов $P_0(t_0)=0.5,\ P_1(t_0)=P_2(t_0)=0,\ P_3(t_0)=0.5$								
Стратегії	$\lambda(t)$	$\lambda^{opt}(t)=0.5906\frac{t}{T^2}$	$0.5906\frac{t}{T^2}$	$0.5906\frac{t}{T^2}$	$0.7382\frac{t}{T^2}$	$0.8858\frac{t}{T^2}$	$1.181\frac{t}{T^2}$	$0.7382\frac{t}{T^2}$
	$\mu(t)$	$\mu^{opt}(t)=0.6299\frac{t}{T^2}$	$0.4724\frac{t}{T^2}$	$0.315\frac{t}{T^2}$	$0.6299\frac{t}{T^2}$	$0.6299\frac{t}{T^2}$	$0.6299\frac{t}{T^2}$	$0.315\frac{t}{T^2}$
Рівень захищеності	I_1	$I_1^{Gar}=0.4055$	0.3761	0.3498	0.3495	0.2806	0.0764	0.2957
Модель ШНП $P_0^{HNP\,opt}(t)=0.6693\left(\frac{t}{T}\right)^2+0.7671\left(\frac{t}{T}\right)^4-0.5541\left(\frac{t}{T}\right)^6$, для умов $P_0(t_0)=P_1(t_0)=P_2(t_0)=0,\ P_3(t_0)=1$								
Стратегії	$\lambda(t)$	$\lambda^{opt}(t)=0.417\frac{t}{T^2}$	$0.417\frac{t}{T^2}$	$0.417\frac{t}{T^2}$	$0.5213\frac{t}{T^2}$	$0.6255\frac{t}{T^2}$	$0.834\frac{t}{T^2}$	$0.6255\frac{t}{T^2}$
	$\mu(t)$	$\mu^{opt}(t)=0.4462\frac{t}{T^2}$	$0.3347\frac{t}{T^2}$	$0.2231\frac{t}{T^2}$	$0.4462\frac{t}{T^2}$	$0.4462\frac{t}{T^2}$	$0.4462\frac{t}{T^2}$	$0.2231\frac{t}{T^2}$
Рівень захищеності	I_1	$I_1^{Gar}=0.1488$	0.1117	0.0758	0.1503	0.155	0.1738	0.0747

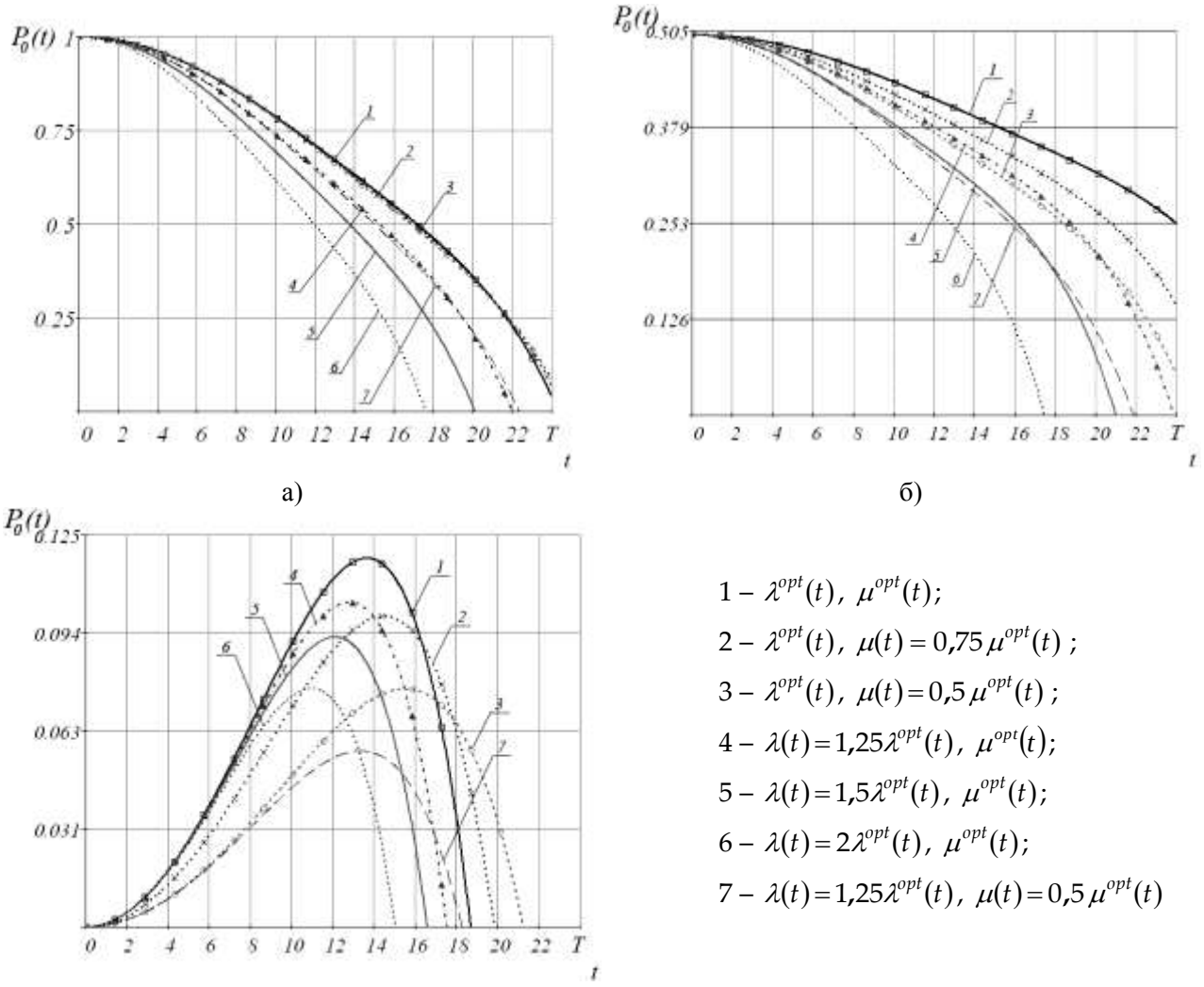

Рис. 4. Моделі шаблонів нормальної поведінки Web-сервера: а) $P_0(t_0)=1$, $P_1(t_0)=P_2(t_0)=P_3(t_0)=0$; б) $P_0(t_0)=0{,}5$, $P_1(t_0)=P_2(t_0)=0$, $P_3(t_0)=0{,}5$; в) $P_0(t_0)=P_1(t_0)=P_2(t_0)=0$, $P_3(t_0)=1$

Висновки та перспективи подальших досліджень

Таким чином, вперше розроблено диференціально-ігрову модель ШНП для Web-серверу для гравця, що атакує, який відрізняється від відомих диференціально-ігровою постановкою задачі моделювання, що дозволяє врахувати динаміку атакуючих дій противника. Це дозволяє гарантовано управляти рівнем захищеності Web-серверу. Аналіз даних, наведених в таблиці та рис. 4, показав, що шаблони нормальної поведінки для Web-серверу відрізняються для різних наборів стратегій гравців 1-7 (рис. 4) та початкових умов. Отже, відхилення супротивником від передбачених стратегій (рис. 4) призводить до відхилення динаміки нормальної поведінки серверу від визначеного шаблону. Найбільш захищеним режимом експлуатації серверу вважається режим, для якого плата I_1 є найменшою. Перспективним напрямом подальших досліджень є моделювання з подальшим отриманням числових характеристик захищеності.

Список літератури:

1. *Atsctoy A.* Самоучитель хакера. — М. : Лучшие книги, 2005. – 192 с.
2. *Мандиа К., Просис К.* Защита от вторжений. Расследование компьютерных преступлений. – М.: ЛОРИ, 2005. – 486 с.
3. *Гостев А., Асеев Е.* Kaspersky Security Bulletin: Основная статистика за 2009 год. – М.: Kaspersky Lab, 2010. – 15 с.
4. *Cisco 2009 Annual Security Report:* Highlighting global security threats and trends / Cisco. – San Jose: Cisco Systems, Inc., 2009. – 40 с.
5. *Андон П. І., Ігнатенко О. П.* Атаки на відмову в мережі Інтернет: опис проблеми та підходів до її вирішення. – К.: Ін-т ПС, 2008. – 52 с..
6. *Ленков С. В. Перегудов Д. А., Хорошко В. А.* Методы и средства защиты информации: в 2-х т. – К.: Арий, 2008. – 464 с.
7. *Аграновский А. В., Хади Р. А.* Новый подход к защите информации – системы обнаружения компьютерных угроз // Информационный бюллетень. – М.: Инфосистемы Джет, 2007. – № 4 (167). – 22 с.
8. *Технології* виявлення вторгнень з використанням шаблонів Data Mining / К. В. Колесніков , В. Ю. Шадхін, Ю. П. Швед та ін. // Вісник ЧДТУ. – Черкаси: ЧДТУ, 2009. – № 1. – С. 15–18.
9. *Андон П. І., Ігнатенко О. П.* Протидія атакам на відмову в мережі Інтернет: концепція підходу // Проблеми програмування. – 2008. – Спеціальний випуск. – С. 564–574.
10. *Бобров А.* Системы обнаружения вторжений [Электронный ресурс] // Intrusion Detection System – IDS. – Режим доступа к журн.: http://www.icmm.ru/~masich/win/lexion/ids/ids.html.
11. *Лошин П.* Обнаружение атак [Электронный ресурс] // Открытые системы. – Режим доступа к журн.: http://www.osp.ru/cw/2001/17/40355.
12. *Защита* информации в компьютерных сетях. Практический курс: учебное пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский и др. Под ред. Н. И. Синадского. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.
13. *Кобозева А. А., Хорошко В.А.* Анализ информационной безопасности. – К.: Изд. ГУИКТ, 2009. – 251 с.
14. *Грищук Р. В.* Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор / Р. В. Грищук // Збірник наукових праць Донецького ІЗТ УДАЗТ. – Донецьк: ДІЗТ, 2009. – № 19. – С. 43–51.
15. *Грищук Р.В.* Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію // Інформаційна безпека. – Луганськ: СНУ ім. В. Даля. – 2009. – № 2(2). – С. 128–132.
16. *Пухов Г. Е.* Дифференциальные спектры и модели. – К.: Наук. думка, 1990. – 184 с.
17. *Терейковський І. А.* Захищеність Web-серверів Apache та IIS // Проблеми програмування. – 2005. – № 2. – С. 42–51.
18. *Воронин А. Н.* Многокритериальный синтез динамических систем. – К.: Наук. думка, 1992. – 160 с.
19. *Бёрд Дж.* Инженерная математика: Карманный справочник: Пер. с англ. – М.: Издательский дом "Додэка-XXI", 2008. – 544 с.