© Lakhno A., Petrenko T., Pyroh M. Modeling of adaptive recognition of cyberattacks in a non-uniform flow of requests in e-business modules // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 2, p. 135-142.

БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ / E-GOVERNANCE SECURITY

МОДЕЛЮВАННЯ РОБОТИ АДАПТИВНОЇ СИСТЕМИ РОЗПІЗНАВАННЯ КІБЕРАТАК В УМОВАХ НЕОДНОРІДНИХ ПОТОКІВ ЗАПИТІВ У МОДУЛЯХ E-BUSINESS

Валерій Лахно[1], Тарас Петренко[2], Микола Пирог[1]

[1]ПВНЗ «Європейський університет», Україна
[2]Чернігівський національний технологічний університет, Україна

ЛАХНО Валерій Анатолійович, д.т.н.

Рік та місце народження: 1964 рік, м. Луганськ, Україна.
Освіта: Луганський машинобудівний інститут (з 2001 року Східноукраїнський Національний університет імені Володимира Даля), 1987 рік.
Посада: завідувач кафедри організації комплексного захисту інформації з 2015 року.
Наукові інтереси: інформаційна безпека, безпека інформаційно-комунікаційних систем.
Публікації: понад 100 наукових публікацій, серед яких монографії, навчальні посібники, підручники, наукові статті та патенти на винаходи.
E-mail: valss21@ukr.net

ПЕТРЕНКО Тарас Анатолійович

Рік та місце народження: 1985 рік, м. Чернігів, Україна.
Посада: старший викладач кафедри математичного моделювання та кібербезпеки
Освіта: Чернігівський державний технологічний університет, 2005 р.
Наукові інтереси: інформаційна безпека, моделювання складних систем, прикладне програмування.
Публікації: 7 наукових публікацій.
E-mail: mail_taras@ukr.net

ПИРОГ Микола Володимирович

Рік та місце народження: 1992 рік, м. Київ, Україна.
Освіта: ПВНЗ «Європейський університет», 2014 рік.
Посада: викладач кафедри інформаційних систем та математичних дисциплін з 2014 року.
Наукові інтереси: кібербезпека, інформаційна безпека держави.
Публікації: 11 наукових публікацій.
E-mail: dart_revan@bigmir.net

Анотація. *Стрімкий розвиток сучасного інформаційного суспільства, зокрема, поширення систем e-business та e-commerce (СЕВ) в різних галузях економіки, викликав певні проблеми із забезпеченням їхньої кібербезпеки, та відповідно, розвиток ринку систем розпізнавання аномалій, кібератак і загроз, що дозволяють виявляти нелегітимні дії атакуючої сторони. Існуючі класичні системи виявлення атак, страждають рядом істотних недоліків, що накладає обмеження на їх практичне використання. Зараз спостерігається тенденція зростання попиту на інтелектуальні технології захисту кіберпростору. Ці технології дозволять побудувати системи розпізнавання кіберзагроз, аномалій та атак на основі машинного навчання і теорії розпізнавання. Отже, потрібні подальші дослідження, спрямовані на розвиток методологічних та теоретичних засад інформаційного синтезу систем кіберзахисту, здатних до самонавчання. Запропоновано математичну модель функціонування адаптивної системи розпізнавання кібератак (АСРК) при неоднорідних потоках запитів та мережних класах кіберзагроз в СЕВ. Встановлено, що Марковські моделі процесів широко використовуються при аналізі й синтезі АСРК, причому властивість марковості є певним обмеженням на викори-*

стовувані реальні сигнали, але цілком достатнім для розробки змістовних методів аналізу й синтезу комплексів АСРК. Визначено, що математичні моделі з використанням апарату ланцюгів Маркова, є ефективним інструментом для кількісної оцінки та розпізнавання складних кібератак із неоднорідними потоками запитів в АСРК.

Ключові слова: *адаптивні системи розпізнавання кібератак, інформаційна безпека, системи e-business, неоднорідні потоки запитів.*

Вступ

Глобальний розвиток комп'ютерних систем e-business та e-commerce (СЕВ) в промисловості, зв'язку на транспорті та ін., вимагає постійного відстеження кіберзагроз, а також уразливостей технічних компонентів і програмного забезпечення. Недосконалість існуючих методів кіберзахисту, а також постійна зміна сценарію дій атакуючої сторони, призводять інформаційні системи (ІС), зокрема й модулі e-business в небезпечний стан. Одним з пріоритетних напрямків захисту, що сприяє своєчасному виявленню кібератак і запобігання їх наслідків для ІС, є шлях розвитку адаптивних систем розпізнавання кібератак (АСРК).

Як показує досвід останніх років, кіберзлочинці все частіше використовують унікальні, ще не відомі ІТ-індустрії, зокрема СЕВ, шкідливі програми, уразливості і способи кібератак. Протистояти постійному зростанню кількості й складності деструктивних впливів на КС можна, зокрема, й використовуючи інтелектуальні АСРК.

Питання про застосування алгоритмів які мають зворотній зв'язок у АСРК, та враховують, наприклад, наявність і розмір черг запитів (кількість запитів у модулях систем електронних накладних, e-business, e-logistics, e-cargo та ін., швидкість надходження запитів (вимог), зокрема з мобільних пристроїв, інтервал між послідовними запитами, тип запиту і т. д.), виникає при більш детальному розгляді моделей розпізнавання нелегітимних дії атакуючої сторони, у яких використовується тільки інформація про вхідні потоки й потоки насичення. У таких випадках раціонально застосовувати інші керуючі моделі та алгоритми розпізнавання, що використовують додаткову інформацію про структуру вхідних потоків запитів, тобто здатних до адоптації та навчання під час виявлення кібератак.

Аналіз існуючих досліджень

У 2015 році спостерігалась тенденція зростання кількості спроб нелегітимного втручання у роботу СЕВ з боку кіберзловмисників, див. рис. 1. Тобто проблематика розвитку систем виявлення кібератак досі є актуальною.

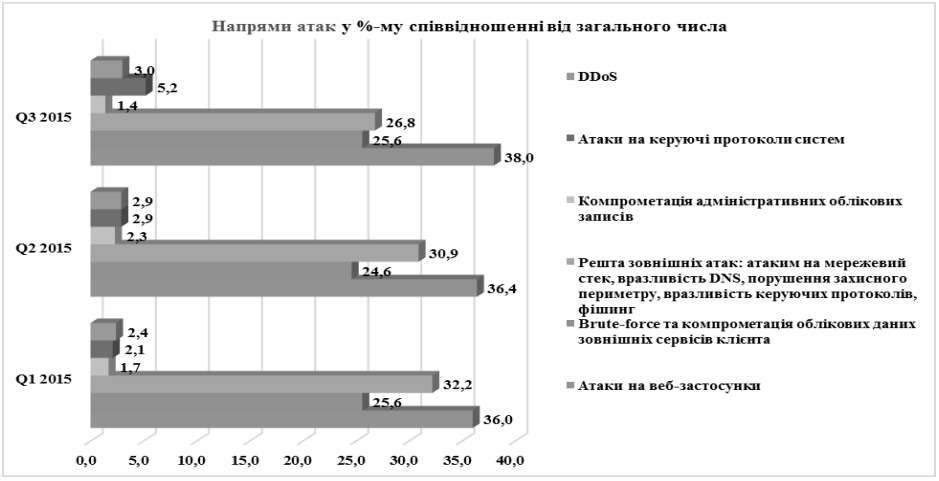


Рис. 1. Розподіл напрямків кібератак на модулі систем e-business за перші три квартали 2015 р. (за даними [21])

Існує досить велика кількість публікацій пов’язаних із розробкою АСРК. Наприклад, в роботах [1-3] міститься ґрунтовний огляд методів виявлення аномалій, а також, запропоновані підходи до класифікації методів виявлення кібератак, що базуються на машинному навчанні і статистичному аналізі дій порушників. Огляд сучасних методів машинного навчання для систем розпізнавання кібератак (СРКА) досить повно представлений в роботах [4-6]. Методи виявлення кібератак на основі кінцевих автоматів (КА) досить докладно викладені в роботах [7, 8]. Іншим перспективним напрямком розвитку АСРК, згадуваним в роботах зарубіжних авторів [9, 10], є напрямок, пов'язаний з виявлення зловживань на основі станів КВКЗ [11].

Методи обчислювального інтелекту, зокрема, нейронні мережі (НС) для задач виявлення кібератак описані в роботах [12, 13]. В [14] описані моделі і методи адаптації генетичних алгоритмів для задачі виявлення кібератак. У роботах [15, 16] описані обчислювальні імунні системи, які можна використовувати для завдання побудови АСОКН. Описана в [17] Баєсова мережа для АСРК – це модель, що дозволяє збирає знімки поведінки КВКЗ кожні кілька секунд для їх подальшого аналізу.

Велика кількість робіт присвячено статистичному аналізу даних у АСРК [1, 2, 18], сигнатурним моделям [2,3] і теоретичним аспектам використання ланцюгів Маркова [5, 6, 19] і мереж Петрі [20] для систем розпізнавання кібератак.

Типовий недолік більшості СРКА, описаних в [11, 16, 18] – помилкові спрацьовування, оскільки в них майже завжди задіяна тільки одна технологія виявлення (як правило, ідентифікація атак). На думку багатьох авторів [5, 8, 10, 20], найперспективнішим напрямом розвитку методів виявлення кібератак і аномалій є об'єднання існуючих підходів в адаптивних гібридних СРКА, що володіють здатністю до самонавчання.

Численні полеміки й публікації [5, 6, 18, 19, 22, 23, 24], пов'язані з розробкою систем кіберзахисту на основі апарату ланцюгів Маркова, а також, використання найрізноманітніших методів і моделей у АСРК, вказують на те, що назріла необхідність удосконалити моделі розпізнавання побудовані із використанням ланцюгів Маркова. Удосконалена модель повинна враховувати можливість використання кіберзлочинцями уразливостей, пов’язаних із неоднорідними потоками запитів у ІС та СЕВ та їхньою втратою внаслідок блокування потоків АСРК при складних цільових кібернападах.

Мета дослідження. Удосконалити математичні моделі розпізнавання для АСРК із неоднорідними потоками запитів у ІС та СЕВ та їхньою втратою внаслідок блокування потоків системами кіберзахисту при складних комп’ютерних атаках.

Основна частина дослідження

Питання про удосконалення моделей розпізнавання складних кібератак за допомогою АСРК виникає при детальнішому розгляді моделей, у яких використовують тільки інформацію про вхідні запити й потоки насичення.

Математичний опис АСРК має наступний вигляд:

$$\Delta =< A\times t\times SW\times KB\times IK, X^{|2|}, B^{|2|}, f_1, f_2 >, \qquad (1)$$

де A – множина вхідних факторів, що підтверджує аномалії або кібератаку (сигналів, ознак), та, що впливає на кібербезпеку ІС та СЕВ; t – множина моментів часу зняття інформації про стан кібербезпеки СЕВ; SW – простір ознак для розпізнавання аномалій та кібератак в СЕВ; KW – простір можливих станів кібербезпеки СЕВ; IK – база знань для ідентифікації аномалій, кіберзагроз або кібератак; $X^{|2|}$ – навчальна матриця (еталон) для класів аномалії та кібератак, що підлягають розпізнаванню (БНМЕ); $B^{|2|}$ – бінарна навчальна матриця, яка переформовується під час навчання; φ_1, φ_2 – оператори формування вхідної та бінарної навчальних матриць відповідно.

Враховуючи наведений опис моделі АСРК, а також, приймаючи до уваги результати висвітлені у роботах [1, 3, 5, 19, 25] подамо ккатегорійну модель АСРК так, див. рис. 2.

Оператор $\Theta: B^{|2|}\to R^{|2|}$ використовується для розбиття простору ознак аномалій, кіберзагроз або кібератак на два класи розпізнавання. За допомогою параметра класифікації $Ą$ перевіряється статистична гіпотеза про приналежність реалізації до класу аномалій, що моделюються, кіберзагроз або кібератак. Оцінюючи стати AS^g, що характеризує точність розпізнавання АСРК, відповідно, q – кількість статистичних гіпотез, $g=q^2$ – кількість характеристик АСРК.

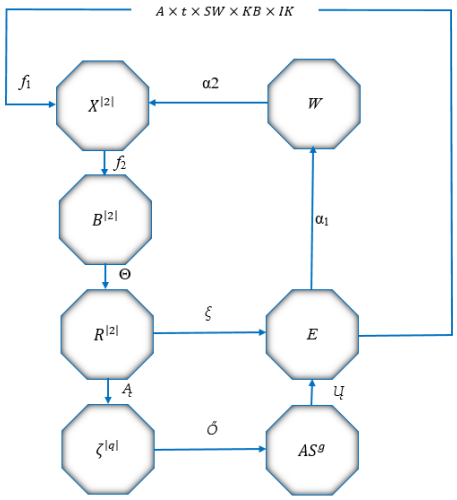


Рис. 2. Категоріальна модель АСРК для СЕВ

Оператор $Ц$ формує множину E, що складається зі значень інформаційного критерія функціональної ефективності АСРК. Оператор ξ використовується для оптимізації системи контрольних відхилень АСРК. Множина W, замикається послідовно оператором $\alpha_1: E\to W$ та оператором $\alpha_2: W\to X$, що змінює реалізації ознак аномалій, кіберзагроз або кібератак в процесі навчання АСРК $\Theta: B^{|2|}\to R^{|2|}$.

Оскільки у загальному випадку методологія розпізнавання кіберзагроз значно відрізняється від методології розпізнавання аномалій та кібератак прийнято припущення, що БНМЕ формуються на попередніх етапах навчання АСРК за рахунок опрацювання великої кількості вимірюваної інформації, наприклад, логи, дані моніторингу та ін.[1, 3, 5, 17, 19, 23, 25].

В рамках статті розглянемо лише дві категорії наведеної моделі – простір можливих станів кібербезпеки СЕВ (KB) та базу знань у формі правил для ідентифікації аномалій, кіберзагроз або кібератак (IK).

Позначимо через N_A множину номерів загроз для кібербезпеки СЕВ; $D_{ззі}$ – множину номерів засобів захисту (ЗЗІ); B_{p_a} – множину номерів загроз, реалізованих порушником при досягненні p_a -ї мети; $N_j^{p_a}$ – множину номерів засобів кіберзахисту (ЗКЗ), які потенційно можна використати для протидії реалізації p_a -ї мети на j -ї лінії захисту (для нейтралізації j -ї загрози, що входить в p_a -у мету) ($p_a=1,2,...PA$; $j=1,2,...,MI$). Причому, $\bigcup_{p_a=1}^{PA} B_{p_a}=N_A$, $n_{p_a}=\left|B_{p_a}\right|$ і $\bigcup_{p_a=1}^{PA}\bigcup_{j\in B_{p_a}}^{n_{p_a}} N_j^{p_a}\subset D_{сзі}$. Отже, процес реалізації порушником кожної зі своїх цілей можна представити у вигляді спрямованого графа (рис. 3).

Вершини графа представляють собою стани СЕВ, що відповідають спробам реалізації порушником деякої кіберзагрози. Стан СЕВ S_0 є початковим, тобто таким, при якому ще жодну із кіберзагроз не реалізовано. Стан S_j ($j \in B_{p_a}$) відповідає спробі реалізації j -ї кіберзагрози. У разі її успішної реалізації, здійснюють перехід до наступного стану СЕВ, а якщо ні, то (при штатному реагуванні ЗКЗ) здійснюють перехід до стану $S_{n_{pa}+1}$ (на рис. 2 $S_{n_{pa}+1} \equiv S_8$).

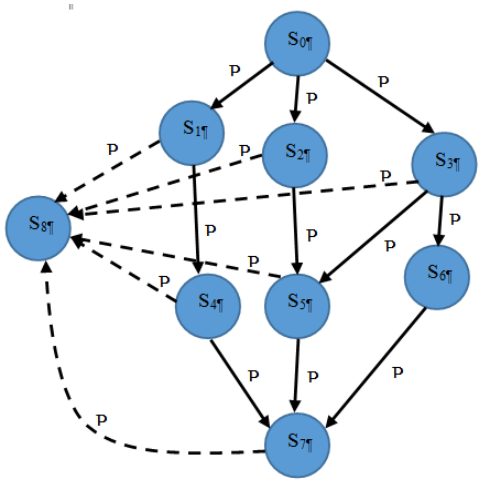


Рис. 3. Стани СЕВ

Стан $S_{n_{pa}}$ є кінцевим і відповідає досягненню порушником p_a -ї мети. Дуги відповідають напрямкам переходів між станами ІС або СЕВ. Кожна дуга характеризує значення імовірності переходу між станами системи. Пунктиром позначено дуги, що відповідають переходу з даного стану в стан $S_{n_{pa}+1}$. Імовірність знаходження системи в *k-му* стані, при спробі реалізації порушником p_a -ї мети, буде визначатися таким виразом:

$$P_k^{p_a} = \sum_{l \in G_{i-1}^{p_a}} P_l^{p_a} p_{lk}^{p_a}, \quad k \in G_i^{p_a},\ i = 0,1,2,...,I^{p_a},\ p_a = 1,2,...,PA, \qquad (2)$$

де I^{p_a} – число рівнів у ранжированому графові станів, що описує діяльність порушника при спробі досягти p_a -ї мети; $G_i^{p_a}$ – множина номерів вершин, що становлять i -й рівень графа станів, що описує діяльність порушника при спробі досягти мети, причому:

$$\bigcup_{i=0}^{I^{p_a}} G_i^{p_a} \subset B_{p_a};\ p_{lk}^{p_a} = \rho_{lk}^{p_a} g_l^{p_a}, \qquad (3)$$

$g_j^{p_a}$ – імовірність подолання j -ї лінії захисту СЕВ при спробі досягнення порушником мети $g_j^{p_a} = \left(1 - e^{-Kq_j K\omega_{p_a}}\right) \prod_{m \in N_j^{p_a}} \left(1 - r_{jm}^{p_a} x_{jm}\right)$; $r_{jm}^{p_a}$ – імовірність успішного функціонування m -го ЗКЗ із протидії діяльності порушника на j -ї лінії СЕВ при спробі досягти ним мети ($j \in B_{p_a}$; $m \in N_j^{p_a}$); – коефіцієнт узгодження при переході системи в j -й стан; $K_{\omega_{p_a}}$ – рівень кваліфікації порушника при спробі досягнення мети, $K_{\omega_{p_a}} \in [0,1]$, при спробі реалізації ним мети, $x_{jm} = \{0,1\}$, x_{jm}=1, якщо m-й засіб використовують на j -ї лінії захисту, x_{jm}=0, а якщо ні, то ($j \in B_{p_a}, j \neq 0, j \neq MI+1$; $m \in N_j^{p_a}$); $\rho_{lk}^{p_a}$ – імовірність переходу з l -го стану в k -й при спробі реалізації порушником мети.

Пропонується наступна модель для АСРК в умовах неоднорідних потоків запитів в СЕВ. Для цього, алгоритм поповнення бази знань та правил, повинен апріорі виділити найбільш значні вхідні потоки запитів, для ідентифікації аномалій, кіберзагроз або кібератак. Ці потоки є найважливіші в сенсі оперативності виконування запитів у ІС або СЕВ. Граф-схема подібної кібератаки наведена на рис. 4.

При стані випадкового оточення (середовища) $c^{(1)}$ запити k_1, k_2, k_3 формують «пачки запитів». Прийнято, що: k_1 – пріоритетний потік запитів із низькою інтенсивністю; k_2 – звичайний потік запитів із низькою інтенсивністю; k_3 – потік запитів найбільшої інтенсивності. Інформативність k_1 – властивість АСРК враховувати наявність запитів у NO_1 (накопичувач) та надходження запитів по цьому потоку, враховуючи динаміку роботи ІС та СЕВ. Пріоритетність k_1 – необхідність пріоритетного виконання запитів, що надійшли у СЕВ. Пріоритетність k_3 – властивість, відповідно до якої, за відсутності запитів до k_1, продовжується виконання запитів k_3.

Відповідним чином організовано роботу обслуговуючого обладнання (ОО, наприклад, серверів СЕВ які оснащені АСРК). Обслуговуюче обладнання перебуває у стані $S^{(r)}, r = \overline{1,7}$, який утворює множину $S = \left\{S^{(r)} : r = \overline{1,7}\right\}$. Обслуговуюче обладнання в стані $S^{(r)}$ перебуває в перебігу часу $\tau_r, r = \overline{1,7}$. Обслуговуюче обладнання виконує функції з аналізу й обслуговування запитів у ІС або СЕВ, а також, керує вхідними потоками та формує черги у NO_1, NO_2, NO_3. Відповідним чином ОО, мають певні стратегії обслуговування – $\alpha_{O1}, \alpha_{O2}, \alpha_{O3}$. Стан $S^{(2j-1)}$ для $j = 1,2,3$ ОО відповідає обслуговуванню запитів потоку k_j. У стані $S^{(2j)}$ для запити k_1, k_2, k_3 не обслуговуються. У стані $S^{(7)}$ обслуговують запити k_3. Згідно із рис. 4, при кожному $r = 1,2,3,4$ стан $S^{(r)}$ зміниться на $S^{(r+1)}$.

Вхідні множини запитів формують в деякому випадковому оточенні (ВО). Приймаємо, що стан ВО визначить імовірнісну конфігурацію для випадків: 1) – множини окремих запитів; 2) – неоднорідні множини запитів («пачки запитів»).

Зазначимо, що S1 – вхід в СЕВ; S2 – сканування доступних ресурсів (ДР) СЕВ; S3 – очікування відповіді про наявність ДР СЕВ; S4 – підключення до ДР; S5 – передавання даних у ІС; S6 – передавання даних на доступні вузли СЕВ; S7 – завантаження відправлення запитів на сервери СЕВ.

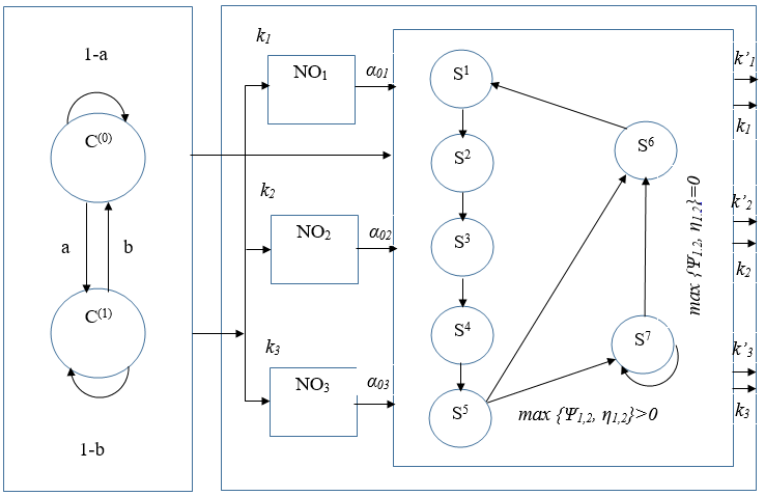


Рис. 4. Функціональна схема кібератаки на СЕВ з неоднорідними потоками запитів

Відповідно до стратегії сторони яка здійснює кібератаку на ІС або СЕВ, вихідні потоки мають мету максимально завантажити систему. При цьому, будь-яким потоком k_i зловмисники, потенційно можуть створювати чергу (приймаємо, що ОО працює без простоїв). Позначимо як k'_1, k'_2, k'_3 множини насичення ІС або СЕВ.

Розглянуто такі варіанти роботи АСРК на СЕВ: 1) кібератаки з посилкою пакетів з нульовою частотою щодо часової шкали часу проходження запитів до адресата й назад; 2) кібератаки, у яких зловмисник може варіювати тривалість імпульсів; 3) атаки з мінімальними випадковими значеннями щодо часової шкали часу проходження запитів до адресата й назад; 4) інші.

Усі аналізовані далі випадкові об'єкти, застосовувані при побудові моделі АСРК та пов'язані із процесом обслуговування запитів у ІС або СЕВ, задано на ймовірнісному просторі $(\Omega, A, \mathrm{P}(*))$ елементарних випадкових подій $\omega \in \Omega$ з імовірнісним заходом $\mathrm{P}(\mathrm{A})$. Опис вхідних потоків запитів здійснено за допомогою нелокального способу. Довільний вхідний потік k_j описують як векторну випадкову послідовність – $\{(\tau_i, \nu_i, \eta_{j,i}); i \geq 0\}$, де $\eta_{j,i}$ – кількість запитів типу ν_i, що надійшли за проміжок часу $[\tau_i, \tau_{i+1})$ цим потоком. Тип запиту визначається міткою ν_i (станом ВО). Поведінку ВО, для простоти, описано однорідною Марковською послідовністю $\{\nu_i; i \geq 0\}$ із двома станами $c^{(0)}$ – потік запитів з малою інтенсивністю, $c^{(1)}$ – великий потік запитів та ймовірностями переходу a, b $0 \leq a < b << 1$. Прийняті обмеження визначать наступні припущення: 1) зміна інтенсивності запитів відбувається рідко; 2) звичайний режим роботи ІС або СЕВ із малоінтенсивним потоком запитів буває частіше, ніж потік з великою кількістю запитів. Ці припущення дають підставу вважати, що за час τ_r, коли ОО перебуває в стані $S^{(r)}$, інтенсивність запитів не зміниться. Змінні пов'язані наступними співвідношеннями:

1. $\nu_{i+1} = \varphi_i(\nu_i, \omega_i)$, де ϕ_i – деякі вимірні уявлення про простір $\{c^{(0)}, c^{(1)}\} \cdot \{0,1\}$ на $\{c^{(0)}, c^{(1)}\}$.

2. $\{\omega_i; i \geq 0\}$ – незалежні випадкові параметри.

Приймаємо, що розподіл цих випадкових параметрів є рівномірним на інтервалі $(0,1)$.

У будь-який момент часу $\tau > 0$ обслуговуюче обладнання перебуває в деякому стані $S(\tau) \in S$. Керування вхідними запитами для СЕВ й зміна станів ОО, враховуючи попередні зауваження, виглядатиме наступним чином:

$$S_{i+1} = u(S_i, \psi_{1,i}, \eta_{1,i}) = \begin{cases} S^{(1)} & при\ S_i = S^{(6)}; \\ S^{(r+1)} & при\ S_i = S^{(r)}\ r = \overline{1,4}; \\ S^{(6)} & при\ S_i \in \{S^{(5)}, S^{(7)}\}\ \&\ \max\{\psi_{1,i}, \eta_{1,i}\} > 0; \\ S^{(7)} & при\ S_i \in \{S^{(5)}, S^{(7)}\}\ \&\ \max\{\psi_{1,i}, \eta_{1,i}\} = 0, \end{cases} \quad (4)$$

де $\psi_{j,i} = \mathrm{f}(w)$ – довжина в NO_j для k_i при $i = 0,1,\ldots k$.

Враховуючи вирішальні правила $\mathrm{gov}(\mathrm{p}_{\mathrm{axi}})\frac{1}{2}$, які визначають стани СЕВ у випадку загроз для кібербезпеки, отримано рекурентні залежності для розпізнавання складних атак у АСРК. Тобто база знань АСПР містить шаблон розпізнавання кібератаки для якої зловмисник створив ситуацію, за якої $S_i \in \{S^{(5)}, S^{(7)}\}$. Таким чином в ОО, наприклад на сервері ІС або СЕВ виконуються запити потоку k_3, при $r = 6$, $y = 0,1; x_{j,k} = \{0,1,...,k\}$. Відповідно, одержимо,

що $Q_{i+1}\left(S^{(6)},c^{(s)},0,w_3,\text{gov}(\text{p}_{\text{axi}})\right)=0$ при всіх $w_3\geq 0$ та $i\geq 0$. При $w_1\geq 1$ отримана наступна залежність:

$$Q_{i+1}\left(S^{(6)},c^{(s)},w_1,0,\text{gov}(\text{p}_{\text{axi}})\right)=\sum_{h=0}^{1}\text{P}_{h,s}\left[\begin{array}{l}\sum_{x=0}^{w_1}\sum_{y=0}^{l_{3,h}}Q_i\left(S^{(5)},c^{(h)},x,y\right)\cdot\varphi_{1,h}\left(w_1-x,\text{T}_5\right)\cdot\sum_{n_3=0}^{l_{3,h}-y}\varphi_{3,h}\left(n_3,\text{T}_5\right)+\\+\sum_{x=0}^{w_1}\sum_{y=0}^{l'_{3,h}}Q_i\left(S^{(7)},c^{(h)},x,y\right)\cdot\varphi_{1,h}\left(w_1-x,\text{T}_7\right)\cdot\sum_{n_3=0}^{l'_{3,h}-y}\varphi_{3,h}\left(n_3,\text{T}_7\right)\end{array}\right], \quad (5)$$

де $l_{1,s},l_{3,s},l'_{3,s}$ – цілі частини параметрів $\mu_{1,s}\text{T}_1,\mu_{3,s}\text{T}_5,\mu_{3,s}\text{T}_7$, $\mu_{j,s}$ – інтенсивність обслуговування запитів потоку k_j, якщо система перебуває в стані $c^{(s)}$ або $c^{(h)}$, а при будь-яких $w_3\geq 1$:

$$Q_{i+1}\left(S^{(6)},c^{(s)},w_1,w_3,\text{gov}(\text{p}_{\text{axi}})\right)=\sum_{h=0}^{1}\text{P}_{h,s}\left[\begin{array}{l}\sum_{x=0}^{w_1}\sum_{y=0}^{w_3+l_{3,h}}Q_i\left(S^{(5)},c^{(h)},x,y\right)\cdot\varphi_{1,h}\left(w_1-x,\text{T}_5\right)\cdot\\\cdot\varphi_{1,h}\left(w_3+l_{3,h}-y,\text{T}_5\right)+\\+\sum_{x=0}^{w_1}\sum_{y=0}^{w_3+l'_3}Q_i\left(S^{(7)},c^{(h)},x,y\right)\cdot\varphi_{1,h}\left(w_1-x,\text{T}_7\right)\cdot\\\cdot\varphi_{1,h}\left(w_3+l'_{3,h}-y,\text{T}_7\right)\end{array}\right]. \quad (6)$$

Для ймовірностей $Q_{i+1}\left(S^{(7)},c^{(s)},w_1,w_3,\text{gov}(\text{p}_{\text{axi}})\right)$ одержимо $Q_{i+1}\left(S^{(7)},c^{(s)},w_1,w_3,\text{gov}(\text{p}_{\text{axi}})\right)=0$ при будь-якому $w_1\geq 0$, $i\geq 0$, $s\in\{1,0\}$:

$$Q_{i+1}\left(S^{(7)},c^{(s)},0,0,\text{gov}(\text{p}_{\text{axi}})\right)=\sum_{h=0}^{1}\text{P}_{h,s}\left[\begin{array}{l}\sum_{y=0}^{l_{3,h}}Q_i\left(S^{(5)},c^{(h)},0,y\right)\cdot\varphi_{1,h}\left(0,\text{T}_5\right)\cdot\sum_{n_3=0}^{l_{3,h}-y}\varphi_{3,h}\left(n_3,\text{T}_5\right)+\\+\sum_{y=0}^{l'_{3,h}}Q_i\left(S^{(7)},c^{(h)},0,y\right)\cdot\varphi_{1,h}\left(0,\text{T}_7\right)\cdot\sum_{n_3=0}^{l'_{3,h}-y}\varphi_{3,h}\left(n_3,\text{T}_7\right)\end{array}\right], \quad (7)$$

а при будь-яких $w_3\geq 0$:

$$Q_{i+1}\left(S^{(7)},c^{(s)},0,w_3,\quad\text{gov}(\text{p}_{\text{axi}})\right)=\sum_{h=0}^{1}\text{P}_{h,s}\left[\begin{array}{l}\sum_{y=0}^{w_3+l_{3,h}}Q_i\left(S^{(5)},c^{(h)},0,y\right)\cdot\varphi_{1,h}\left(0,\text{T}_5\right)\cdot\varphi_{3,h}\left(w_3+l_{3,h}-y,\text{T}_5\right)+\\+\sum_{y=0}^{w_3+l'_{3,h}}Q_i\left(S^{(7)},c^{(h)},0,y\right)\cdot\varphi_{1,h}\left(0,\text{T}_7\right)\cdot\varphi_{3,h}\left(w_3+l'_{3,h}-y,\text{T}_7\right)\end{array}\right]. \quad (8)$$

Перехідні ймовірності на кожному кроці ітераційної процедури визначення параметрів ймовірності реалізації атаки визначаються на підставі методів мультифрактального та кластерного аналізу, а також показника Херста [3, 5, 19, 23]. Крім того, використовуються результати отримані на попередніх стадіях формування бінарних навчальних матриць для аномалій та кібератак [25]. Результати тестування запропонованої моделі для АСРК у СЕВ показані далі.

Результати дослідження

На рис. 5, 6 показано основні результати моделювання неоднорідних потоків запитів k_1,k_2,k_3 у ІС та СЕВ. Отже, при створенні пріоритетних неоднорідних потоків запитів, час опрацювання даних у ІС або СЕВ збільшується у 1,5-3,5 рази.

Отже, для проведення успішної кібератаки на СЕВ, зокрема типу «відмова в обслуговуванні», не обов'язково створювати велику кількість запитів до сервера або знижувати смугу пропускання трафіка. Можна з досить високим ступенем ймовірності успіху експлуатувати уразливості, пов'язані зі створенням малоінтенсивного пріоритетного потоку, наприклад, варіюючи такими параметрами, як швидкість пакета (низькошвидкісні атаки); кількість пакетів з нульовою частотою щодо RTT; тривалість імпульсу та ін.

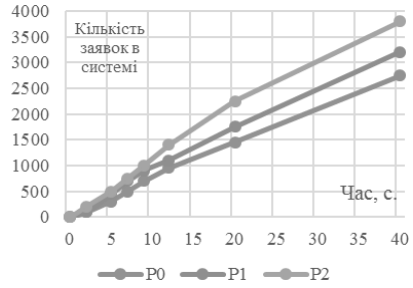
Модель розпізнавання складних кібератак для АСРК, з урахуванням можливостей зміни нападаючими інтенсивності неоднорідних потоків запитів, доведено до практичної реалізації створенням відповідних програмних модулів експертної системи «Аналізатор загроз», що дозволяє підвищити ефективність розпізнавання загроз для кібербезпеки СЕВ до 85-98 %.

Висновки

Основні результати досліджень полягають у такому:

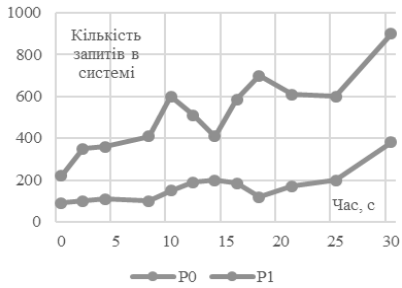
1. Запропоновано математичну модель для адаптивної системи розпізнавання кібератак у ІС або СЕВ яка враховує можливість створення атакуючим неоднорідних потоків запитів при мережних класах кібератак. Показано, що математичні моделі із використанням апарату ланцюгів Маркова є дієвим інструментом для кількісного оцінювання можливості реалізації кібератак у СЕВ.

2. Синтезовано моделі програмних атак у СЕВ, які, на відміну від існуючих, враховують неоднорідні вхідні потоки запитів, враховують наявність їх черг та апріорі виділяють найінтенсивніші вхідні потоки, що дозволяє здійснювати вибір способів протидії та нейтралізацію наслідків від їх впливу, аналізувати більш складні і раніше невідомі види програмних атак.



P0 – без атаки; P1, P2 – кібератака відмова у обслуговуванні;

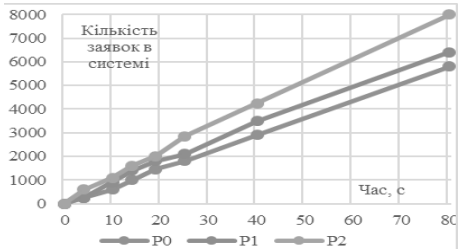
а) сумарний потік запитів.



P0 – без атаки; P1 – кібератака відмова у обслуговуванні;

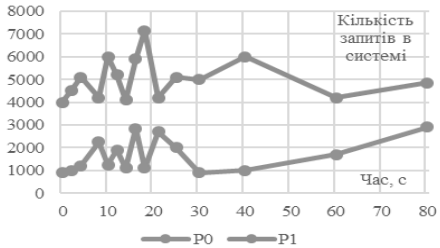
б) середній потік запитів.

Рис. 5. Розподіл сумарного й середнього потоку окремих запитів у СЕВ



P0 – без атаки; P1, P2 – кібератака відмова у обслуговуванні;

а) сумарний потік запитів.



P0 – без атаки; P1 – кібератака відмова у обслуговуванні;

б) середній потік запитів.

Рис. 6. Розподіл сумарного й середнього потоку запитів при створенні неоднорідного потоку та розпізнаванні загрози КНІ

Література

[1] Jyothsna V., Prasad Rama V.V. A review of anomaly based intrusion detection systems. International Journal of Computer Applications, Vol. 28, No. 7. P. 26–35. DOI: 10.5120/3399-4730.

[2] Baddar S.A.-H., Merlo A., Migliardi M. Anomaly detection in computer networks: a state-of-the-art review. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 5, No. 4. P. 29-64.

[3] Gyanchandani M., Rana J.L., Yadav R.N. Taxonomy of anomaly based intrusion detection system: a review. International Journal of Scientific and Research Publications, Vol. 2, Iss. 12. P. 1-13.

[4] Vinchurkar D.P., Reshamwala A. A review of intrusion detection system using neural network and machine learning technique. International Journal of Engineering Science and Innovative Technology (IJESIT), Vol. 1, Iss. 2. P. 54-63.

[5] Tsai C.-F., Hsub Y.-F., Linc C.-Y., Lin W.-Y. (2009). Intrusion detection by machine learning: a review. Expert Systems with Applications, Vol. 36, Iss. 10. P. 11994-12000. DOI: 10.1016/j.eswa.2009.05.029.

[6] Omar S., Ngadi A., Jebur H.H. Machine learning techniques for anomaly detection: an overview. International Journal of Computer Applications, 2013. Vol. 79, No. 2. P. 33-41. DOI:10.5120/13715-1478.

[7] Ilgun K., Kemmerer R.A., Porras P.A. State transition analysis: a rule-based intrusion detection approach. IEEE Transactions on Software Engineering, 1995. Vol. 21, Iss. 3. P. 181-199.

[8] Khan L., Awad M., Thuraisingham B. A new intrusion detection system using support vector machines and hierarchical clustering. The International Journal on Very Large Data Bases, Vol. 16, Iss. 4, P. 507-521. DOI: 10.1007/s00778-006-0002-5.

[9] Wu S.X., Banzhaf W. The use of computational intelligence in intrusion detection systems: a review. Applied Soft Computing, Vol. 10, Iss. 1. P. 1–35. DOI: 10.1016/j.asoc.2009.06.019.

[10] Kabiri P., Ghorbani A.A. Research on intrusion detection and response: a survey. International Journal of Network Security, 2005. Vol. 1, No. 2. P. 84-102.

[11] Ameziane El Hassani, A., Abou El Kalam, A., Bouhoula, A., Abassi, R., Ait Ouahman, A. Integrity-OrBAC: a new model to preserve Critical Infrastructures integrity. International Journal of Information Security, 14 (4), 367-385.

[12] Al-Jarrah O., Arafat A. Network Intrusion Detection System using attack behavior classification. Information and Communication Systems (ICICS), 2014 5th International Conference, p.1-6. DOI: 10.1109/IACS.2014.6841978.

[13] Selim S., Hashem M., Nazmy T. M. Detection using multi-stage neural network. International Journal of Computer Science and Information Security, 2010. Vol. 8, No. 4. P. 14-20.

[14] Pawar S.N. Intrusion detection in computer network using genetic algorithm approach: a survey. International Journal of Advances in Engineering Technology, 2013. Vol. 6, Iss. 2. P. 730–736.

[15] Zhou Y.P. Hybrid Model Based on Artificial Immune System and PCA Neural Networks for Intrusion Detection. Asia-Pacific Conference on

Information Processing, 2009, Vol. 1, P. 21-24. DOI:10.1109/APCIP.2009.13.

[16] Komar M., Golovko V., Sachenko A., Bezobrazov S. Development of Neural Network Immune Detectors for Computer Attacks Recognition and Classification. IEEE 7th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013. Vol. 2. P. 665-668. DOI: 10.1109/ IDAACS.2013.6663008.

[17] Heckerman D. A tutorial on learning with bayesian networks. Innovations in Bayesian Networks: Theory and Applications, 2008. Vol. 156. P. 33-82. DOI:10.1007/978-3-540-85066-3_3.

[18] Zhan Z., Xu M., Xu S. Characterizing Honeypot-Captured Cyber Attacks: Statistical Framework and Case Study. IEEE Transactions on Information Forensics and Security, Vol. 8, Iss. 11, P. 1775 – 1789. DOI: 10.1109/TIFS.2013.2279800.

[19] Raiyn J. A survey of Cyber Attack Detection Strategies. International Journal of Security and Its Applications, Vol.8, No.1, P. 247-256. DOI:/10.14257/ijsia.2014.8.1.23.

[20] Bartosz Jasiul, Marcin Szpyrka, Joanna Śliwa. Detection and Modeling of Cyber Attacks with Petri Nets. Entropy, 16(12), pp. 6602-6623; DOI:10.3390/e16126602.

[21] Attacks Statistics 2015 [Electronic resource]. – Available at:http://www.hackmageddon.com/2016/ 01/11/2015-cyber-attacks-statistics/.

[22] Харин, Ю. С. Алгоритмы статистического анализа цепей Маркова с условной глубиной памяти / Ю. С. Харин, М. В. Мальцев // Информатика. – 2011. – №1. – С.34-43.

[23] Щерба М.В. Методика разработки системы защиты информации комплекса муниципальных информационных систем [Текст] / М.В. Щерба // Информационные технологии моделирования и управления. – 2009. – Вып. 6(58). – С. 850-854.

[24] Евсютин О.О. Моделирование в информационной безопасности и обработке данных с использованием математического аппарата дискретных динамических систем [Текст] / О.О. Евсютин, В.Г. Миронова // Ползуновский вестник. – 2012. – № 3/2. – С. 222-226.

[25] Lakhno V. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features [Text] / V. Lakhno, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko, T. Zhmurko // Eastern-European Journal of Enterprise Tech. – 2016. – № 3/9 (81). – P. 30-38.

УДК 004.056 (045)

Лахно А.В., Петренко Т.А., Пирог М.В. Моделирование работы адаптивной системы распознавания кибератак в условиях неоднородных потоков запросов в модулях e-business

Аннотация. *Стремительное развитие современного информационного общества, в частности, распространение систем e-business и e-commerce (СЕВ) в различных отраслях экономики, вызвало определенные проблемы с обеспечением их кибербезопасности, и соответственно, развитие рынка систем распознавания аномалий, кибератак и угроз, позволяющие выявлять нелегитимные действия атакующей стороны. Существующие классические системы обнаружения атак, страдают рядом существенных недостатков, что накладывает ограничения на их практическое использование. Сейчас наблюдается тенденция роста спроса на интеллектуальные технологии защиты киберпространства, способные моделировать когнитивные процессы и построены на основе машинного обучения и теории распознавания. Значит, нужны дальнейшие исследования, направленные на развитие методологических и теоретических основ информационного синтеза систем киберзащиты, способных к самообучению. Предложена математическая модель функционирования адаптивной системы распознавания кибератак (АСРК) при неоднородных потоках запросов и сетевых классах киберугроз в СЕВ. Установлено, что Марковские модели процессов широко используются при анализе и синтезе АСРК, причем свойство марковости является определенным ограничением на используемые реальные сигналы, но вполне достаточным для разработки содержательных методов анализа и синтеза комплексов АСРК. Определено, что математические модели с использованием аппарата цепей Маркова, является эффективным инструментом для количественной оценки и распознавания сложных кибератак с неоднородными потоками запросов в АСРК.*

Ключевые слова*: адаптивные системы распознавания кибератак, информационная безопасность, системы e-business, неоднородные потоки запросов.*

Lakhno A., Petrenko T., Pyroh M. Modeling of adaptive recognition of cyberattacks in a non-uniform flow of requests in e-business modules

Abstract. *The rapid development of modern information society, in particular, distribution systems, e-business and e-commerce (CEB) in various sectors of the economy, has caused some problems with the provision of cyber security, and accordingly, the development of the market anomaly detection systems, cyberattacks and threats that identify illegitimate action attacking side. Existing classic intrusion detection systems, suffer from a number of significant deficiencies, which imposes restrictions on their practical use. Now there is a trend of growth in demand for intelligent security technology of cyberspace, capable of simulating cognitive processes and are based on machine learning and pattern recognition theory. Hence, we need further research to develop the methodological and theoretical foundations of information synthesis cyber defense systems capable of self-learning. A mathematical model of adaptive functioning of cyberattacks recognition system (ACRS) at a non-uniform flow of network requests and cyber classes in CEB. It was found that the Markov process models are widely used in the analysis and synthesis of ACRS, the Markov property is a certain limitation on the real signals, but it is sufficient for the development of methods of content analysis and synthesis ACRS complexes. It was determined that the mathematical models using Markov chain device is an effective tool for quantitative assessment and recognition of complex cyberattacks with non-uniform flow of requests in ACRS.*

Key words*: recognition adaptive systems of cyber attacks, information security, e - business systems, non-uniform flow of requests.*

Отримано *1 квітня 2016 року*, затверджено редколегією *14 квітня 2016 року*