DOI: 10.18372/2410-7840.20.12655
УДК 004.41:004.056

GERT-МЕРЕЖЕВИЙ СИНТЕЗ ТЕХНОЛОГІЇ ТЕСТУВАННЯ НА ВРАЗЛИВІСТЬ WEB-ДОДАТКІВ

Олександр Коваленко

В роботі представлені результати дослідження та алгоритми тестування на вразливість до одних з найбільш поширених видів атак на Web-додатки - DOM XSS і SQL ін'єкції. Аргументовано обраний підхід математичного моделювання на основі GERT-мереж. Розроблено комплекс математичних моделей технології тестування Web-додатків. В основу математичного моделювання покладено підхід GERT-мережевого синтезу. В результаті розроблено математичні моделі технології тестування DOM XSS уразливості і технології тестування уразливості до SQL ін'єкцій. Математична модель технології тестування DOM XSS уразливості відрізняється від відомих, урахуванням виконання або аналізу DOM структури. Математична модель технології тестування уразливості до SQL ін'єкцій відрізняється від відомих, вдосконаленим способом визначення відстані між результатами ін'єкції.

Ключові слова: *атаки на Web-додатки, DOM XSS, SQL ін'єкції, GERT-мережі.*

АНАЛІЗ ЛІТЕРАТУРИ І ПОСТАНОВКА ЗАДАЧІ. В даний час великий попит на Web-додатки і Web-послуги обумовлює великий інтерес зловмисників до їх можливих вразливостей. При цьому основні загрози в напрямку серверних компонентів трансформується в атаки, спрямовані проти звичайних користувачів.

Проведений аналіз матеріалів Open Web Application Security Project (OWASP TOP-10) показав, що одним з найбільш небезпечних видів атак (вразливостей) є міжсайтовий скриптинг – XSS (Cross Site Scripting).

Аналіз літератури показав, що міжсайтовий скриптинг це помилка валідації призначених для користувача даних, яка дозволяє передати JavaScript код на виконання в браузер користувача. Атаки такого роду часто також називають HTML-ін'єкціями, адже механізм їх впровадження дуже схожий з SQL-ін'єкціями, але на відміну від останніх, впроваджуваний код виповнюється в браузері користувача.

З робіт [1, 6-9] відомо, що під XSS зазвичай мається на увазі моментальний і відкладений міжсайтовий скриптинг. При моментальному XSS зі шкідливим кодом (Javascript) повертається атакується сервером негайно як відповідь на HTTP запит. Відкладений XSS означає, що ця шкідлива програма зберігається на атакуємій системі і пізніше може бути впроваджена в HTML сторінку вразливої системи. Така класифікація передбачає, що фундаментальна властивість XSS полягає в тому, що це шкідлива програма відсилається з браузера на сервер і повертається в цей же браузер (моментальний XSS) або будь-який інший браузер (відкладений XSS).

У ряді інтернет-статей докладно описані основні механізми виникнення подібного роду погроз, а також шляхи можливого блокування. Однак, щоб ідентифікувати ці загрози і можливі наслідки їх поширення в процесі безпечного управління IT-проектами, а також запропонувати оптимальні шляхи вирішення цієї проблеми, існує необхідність математичної формалізації процесу їх ініціалізації і поширення.

Особливо актуальним завданням в цьому напрямку є моделювання DOM (Document Object Model) XSS уразливості. Пов'язано це з тим, що уразливість DOM XSS є підвид XSS, в разі якої результат атаки знаходиться не у відповіді сервера і, відповідно, не в HTML коді, а в DOM структурі HTML сторінки. Результати атак за допомогою таких вразливостей можна виявити тільки в процесі виконання або аналізі DOM структури. Сам механізм атаки, а саме ін'єкція Javascript коду у вразливий сегмент, залишається незмінним.

МАТЕМАТИЧНА МОДЕЛЬ ТЕХНОЛОГІЇ ТЕСТУВАННЯ КОМПЛЕКСУ DOM XSS ВРАЗЛИВОСТЕЙ. Для математичної формалізації алгоритму виявлення комплексу DOM XSS вразливостей різних типів скористаємося основними положеннями мережевого GERT-моделювання, докладно описаними в роботах [1, 6, 7].

Проведені дослідження показали, що GERT (Graphical Evaluation and Review Technique) - є методом вивчення та аналізу стохастичних мереж, які використовуються для опису логічного взаємозв'язку між частинами проекту або етапами процесу [6]. Головною метою GERT є оцінка логіки мережі і тривалість активності і отримання висновку про необхідність виконання деяких активностей.

Мережі GERT складаються з вузлів типу AND, INCLUSIVE-OR і EXCLUSIVE-OR, і гілок з двома і більше параметрами. Гілка, має напрямок, має вузол початку і вузол кінця.

В цілому, проведені дослідження показали, що GERT-моделювання є ефективним способом визначення заздалегідь невідомих законів і функцій розподілу випадкових величин при відомому алгоритмі функціонування (процесу). Саме тому, як інструмент математичного моделювання нами було вибрано GERT-моделювання.

Побудуємо, відповідно до представленого описом мережеву GERT-модель технології тестування комплексу DOM XSS вразливостей. Графічне зображення GERT-моделі представлено на рис. 1.

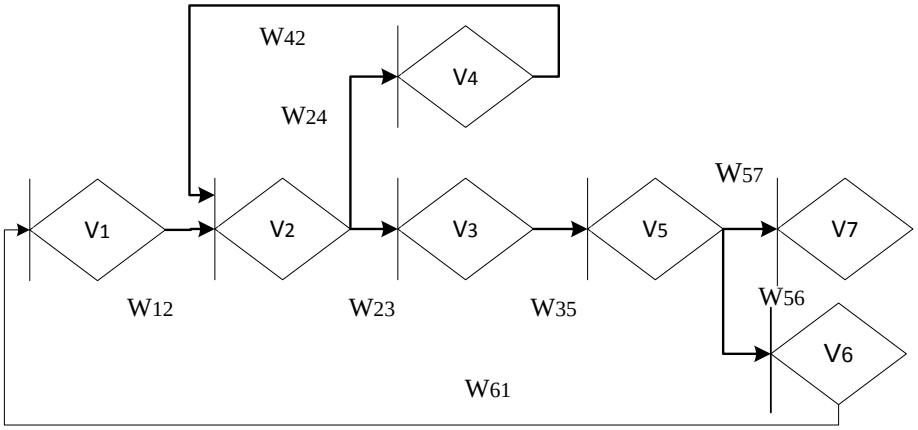

Рис. 1. GERT-модель технології тестування комплексу DOM XSS вразливостей

У представленій мережі вузли графа інтерпретуються станами комп'ютерної системи в процесі функціонування DOM структури, а гілки графа – ймовірносно-тимчасовими характеристиками переходів між станами. Зокрема гілка (1,2) описує процес отримання та аналізу вмісту тега. Гілка (2,3) відображає процес виконання атаки в разі наявності «Source» структури. Гілка (2,4) визначається процедурами звернення до вмісту віддаленого файлу (пошук «sink»). Гілка (4,2) характеризує повернення на виконання атаки. Гілка (3,5) описує продовження атаки, зокрема перевірку вмісту DOM. Гілка (5,6) характеризує одну з основних особливостей аналізу алгоритму XXS вразливостей різних типів - автоматичний аудит коду (при необхідності віддалений). Гілка (5,1) відображає процес переходу до нового тегу. Далі гілка (5,7) характеризує заключну стадію прийняття рішення про уразливість

Еквівалентна W-функція часу виконання алгоритму тестування комплексу DOM XSS різних типів (в тому числі DOM Based XSS) вразливостей дорівнює:

$$W_E(s)=\frac{W_{12}W_{23}W_{35}W_{56}+W_{12}W_{24}W_{42}W_{23}W_{35}W_{57}}{1-W_{12}W_{23}W_{35}W_{51}-W_{12}W_{24}W_{42}W_{23}W_{35}W_{56}W_{61}}=$$

$$=\frac{p_1p_2^2\lambda_1\lambda_2^2\left(p_4\lambda_4(\lambda_3-s)^2(\lambda_5-s)+p_3^2q_1\lambda_3^2\lambda_5(\lambda_4-s)\right)}{(\lambda_4-s)\left((\lambda_1-s)(\lambda_2-s)^2(\lambda_3-s)^2(\lambda_5-s)-\right.}, \quad (1)$$

$$\left.-p_1\lambda_1p_2^2\lambda_2^2q_1\lambda_5(\lambda_3-s)^2-p_1p_2^2p_3^2p_4\lambda_1\lambda_2^2q_1\lambda_3^2\lambda_4\lambda_5\right)$$

де $1-p_4=q_1$.

Особливість даного процесу полягає в різнорідності аналізованих і оброблюваних даних. При цьому можливі різні випадки організації зворотного зв'язку.

Для GERT-мереж з циклами не існує простих методів знаходження особливих точок $\Phi_E(z)$ функції заміни дійсних змінних $(z=-i\varsigma)$, де ς - дійсна змінна. Це пояснюється тим, що для знаходження особливих точок необхідно вирішувати нелінійні рівняння, і чим складніше структура GERT-мережі, тим складніше і вихідне рівняння. Тому в ході моделювання пропонується вдатися до подібної заміни.

Виконуючи комплексне перетворення $z=-s$, отримаємо

$$\Phi(z)=\frac{uz^3+vz^2+bz+k}{(\lambda_4+z)\left(z^6+cz^5+dz^4+gz^3+hz^2+wz+m\right)}, \quad (2)$$

де $u=-p_1p_2^2p_4\lambda_1\lambda_2^2\lambda_4$, $v=p_1p_2^2p_4\lambda_1\lambda_2^2\lambda_4(\lambda_5+2\lambda_3)$, $b=-p_1p_2^2p_4\lambda_1\lambda_2^2\lambda_4\lambda_3(2\lambda_5-\lambda_3)$, $k=-p_1p_2^2\lambda_1\lambda_2^2\lambda_3^2\lambda_4\lambda_5\left(p_4+p_3^2q_1\right)$, $c=\lambda_1+2\lambda_2+2\lambda_3+\lambda_4+\lambda_5$, $d=-(2\lambda_3\lambda_5\lambda_4+\lambda_1\lambda_5\lambda_4+2\lambda_2\lambda_5\lambda_4+\lambda_3^2+2\lambda_1\lambda_3+4\lambda_2\lambda_3+2\lambda_1\lambda_2+\lambda_2^2)$,

$$g=\left(\begin{matrix}\lambda_3^2\lambda_4\lambda_5+4\lambda_1\lambda_2\lambda_4\lambda_5+4\lambda_2\lambda_3\lambda_4\lambda_5+\lambda_2^2+\lambda_3^2\lambda_1+2\lambda_3^2\lambda_2+4\lambda_1\lambda_2\lambda_3\lambda_4+\\+2\lambda_2^2\lambda_3+\lambda_2^2\lambda_1+\lambda_3^2\lambda_4+\lambda_2^2\lambda_4\end{matrix}\right),$$

$$h=-\left(\begin{matrix}\lambda_1\lambda_3^2\lambda_4\lambda_5+2\lambda_2\lambda_3^2\lambda_4\lambda_5+4\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5+2\lambda_2^2\lambda_3\lambda_4\lambda_5+\lambda_2^2\lambda_3^2\lambda_4+\\+2\lambda_1\lambda_2^2\lambda_3\lambda_4-p_1p_2^2p\ q_1\lambda_1\lambda_2\lambda_4\lambda_5\end{matrix}\right),$$

$$w=\lambda_1\lambda_2\lambda_3^2\lambda_4\lambda_5+\lambda_2^2\lambda_3^2\lambda_4\lambda_5+2\lambda_1\lambda_2^2\lambda_3\lambda_4\lambda_5+\lambda_1\lambda_2^2\lambda_4\lambda_3-2p_1p_2^2p_4q_1\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5,$$

$$m=p_1p_2^2p_4q_1\lambda_1\lambda_2\lambda_3^2\lambda_4\lambda_5+p_1p_2^2p_3p_4q_1\lambda_1\lambda_2^2\lambda_3^2\lambda_4\lambda_5-\lambda_1\lambda_2^2\lambda_3\lambda_4\lambda_5.$$

Щільність розподілу ймовірностей часу виконання алгоритму аналізу DOM XSS вразливості:

$$\varphi(x)=\frac{1}{2\pi i}\int_{-i\infty}^{i\infty} e^{zx}\frac{uz^3+vz^2+bz+k}{\left(z^6+cz^5+dz^4+gz^3+hz^2+wz+m\right)}dz, \quad (3)$$

де операція інтегрування виконується за допомогою інтегралу Бромвича-Вагнера [6]

Спосіб інтегрування залежить від того, чи має функція $\Phi(z)$ лише прості полюси, чи полюси деякого порядку. В тому числі, коли функція $\Phi(z)$ має лише прості полюси, вираз $e^{zx}\Phi(z)$ можна представити у вигляді:

$$e^{zx}\Phi(z)=\frac{e^{zx}\left(uz^3+vz^2+bz+k\right)}{z^7+\gamma_6 z^6+\gamma_5 z^5+\gamma_4 z^4+\gamma_3 z^3+\gamma_2 z^2+\gamma_1 z+\gamma_0}=\frac{\mu(z)}{\psi(z)}, \quad (4)$$

де $\gamma_6=c$, $\gamma_5=c+d$, $\gamma_4=d+g$, $\gamma_3=g+h$, $\gamma_2=h+w$, $\gamma_1=w+m$, $\gamma_0=m$.

Тоді щільність розподілу часу виконання алгоритму аналізу DOM XSS вразливості всіх типів дорівнює:

$$\phi(x)=\sum_{k=1}^{7}\operatorname{Res}\left[e^{zx}\Phi(z)\right]=\sum_{k=1}^{7}\frac{\mu(z_k)}{\psi(z_k)}=\sum_{k=1}^{7}\frac{e^{zx}\left(uz^3+vz^2+bz+k\right)}{7z_k^6+6\gamma_6 z_k^5+5\gamma_5 z_k^4+4\gamma_4 z_k^3+3\gamma_3 z_k^2+2\gamma_2 z_k+\gamma_1}. \quad (5)$$

Функція $\Phi(z)$ крім рішень, що визначають коренями управління $z^6+cz^5+dz^4+gz^3+hz^2+wz+m=0$, може мати і полюс другого чи третього порядку. Тоді щільність розподілу часу передачі повідомлення $\varphi(x)$ знаходиться за формулою знаходження відрахувань r_{-1} від полюсів z_k порядку n:

$$r_{-1}=\frac{1}{(n-1)!}\lim_{z\to z_k}\frac{d^{n-1}\left((z-z_k)^n e^{zx}\Phi(z)\right)}{dz^{n-1}}. \quad (6)$$

Вираз (6) являє собою дробово-раціональну функцію щодо z зі ступенем знаменника більшим, ніж ступінь чисельника. Тому для нього виконується умови леми Жордана [6].

Багаточлен $z^6+cz^5+dz^4+gz^3+hz^2+wz+m$ породжує сім полюсів. Рішення рівняння

$$z^6+cz^5+dz^4+gz^3+hz^2+wz+m=0 \quad (7)$$

може бути знайдено будь-яким методом, наприклад, по формулам Вієта [6]. В результаті обчислюються особливі точки z_1, z_2, z_3, z_4, z_5, z_6.

Таким чином, на основі експоненційної GERT-мережі розроблено математичну модель технології тестування комплексу DOM XSS вразливостей всіх типів («stored XSS», «reflected XSS» і DOM Based XSS), яка відрізняється від відомих, урахуванням їх специфіки та необхідності автоматичного аудиту DOM Based XSS окремо.

Розроблена модель може бути використана для дослідження Інтернет WordWeb-додатків в мережевих структурах, а також при розробці нових засобів і протоколів захисту даних в комп'ютерних системах і мережах.

Застосування експоненційних стохастичних моделей GERT дасть можливість використання результатів, отриманих в аналітичному вигляді (функції, щільності розподілу) для проведення порівняльного аналізу і досліджень, більш складних комп'ютерних систем математичними методами.

ДОСЛІДЖЕННЯ GERT-МОДЕЛІ ТЕХНОЛОГІЇ ТЕСТУВАННЯ КОМПЛЕКСУ DOM XSS ВРАЗЛИВОСТЕЙ. Розглянемо приклад XSS атаки через DOM (аналогічний алгоритм простого використання клієнтського скрипта для (небезпечної) переадресації браузера до іншого ресурсу).

Знайдемо щільності розподілу $\varphi(x)$ ймовірностей часу виконання алгоритму за умови, що z вибираються як корені рівняння $(z^6+cz^5+dz^4+gz^3+hz^2+wz+m)=0$, умовні ймовірності та інтенсивності в гілках *GERT*-мережі мають значення: $p_1=0{,}999$, $p_2=0{,}6$, $p_3=0{,}4$, $p_4=0{,}99$, $\lambda_1=0{,}9999$, $\lambda_2=0{,}79$, $\lambda_3=0{,}29$, $\lambda_4=0{,}39$.

З урахуванням наведених ознак GERT-мережі, відповідно до виразу (2), а так само використовуючи спеціалізований математичний пакет Mathcad, отримаємо, що в знаменнику виразу (3) сформований поліном

$$x^6+4{,}07x^5-6{,}66x^4+6{,}529x^3-1{,}592x^2+0{,}617x-0{,}164=0. \quad (8)$$

Корені цього полінома (і відповідно функції $\Phi(z)$) дорівнюють:

x1 ≈ -5,50538139377208, (P(x1) ≈ 0; iter = 1);

x2 ≈ -0,0498463517249773 + i · 0,331259064468874, (P(x2) ≈ -0,000162 - i · 0,00073; iter = 3);

x3 ≈ -0,0495665029547472 - i · 0,331246931512067, (P(x3) ≈ −0,000307 + i · 0,00013; iter = 3);

x4 ≈ 0,28764249382953 − i · 0,000140961065526, (P(x4) ≈ 0,000129 − i · 0,000118; iter = 3);

x5 ≈ 0,623543971678568 − i · 0,731454207007899, (P(x5) ≈ 0; iter = 3);

x6 ≈ 0,623607782943707 + i · 0,731584150633824, (P(x6) ≈ 0; iter = 2).

Досліджуємо залежність функції $\Phi(z)$ від інтенсивності λ_2, що є одним з основних показників в даному алгоритмі (інтенсивність λ_2 характеризує виконання атаки в разі наявності «Source» структури).

На рис. 2 представлена крива графіка залежності функції $\Phi(z)$ від інтенсивності λ_2 в розглянутих вище умовах. Як видно з малюнка випадкова величина λ_2 розподілена відповідно до показовим законом.

Використовуючи отримані значення, знайдемо $\varphi(x)$. Відповідно до формули (5) $\varphi(x)$ дорівнює:

$$\phi(x)=\sum_{k=1}^{6}\operatorname{Res}_{z=z_k}\left[e^{zx}\Phi(z)\right]=$$

$$=\frac{e^{(a+\delta i)x}\left(u(a+\delta i)^3+v(a+\delta i)^2+b(a+\delta i)+k\right)}{\left(\begin{array}{l}7(a+\delta i)^6+6g_6(a+\delta i)^5+5g_5(a+\delta i)^4+4g_4(a+\delta i)^3+3g_3(a+\delta i)^2+\\+2g_2(a+\delta i)+g_1\end{array}\right)}-$$

$$-\frac{e^{(a-bi)x}\left(u(a-\delta i)^3+v(a-\delta i)^2+b(a-\delta i)+k\right)}{\left(\begin{array}{l}7(a-\delta i)^6+6g_6(a-\delta i)^5+5g_5(a-\delta i)^4+4g_4(a-\delta i)^3+3g_3(a-\delta i)^2+\\+2g_2(a-\delta i)+g_1\end{array}\right)}. \quad (9)$$

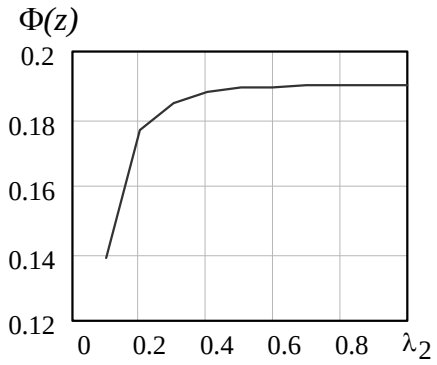

Рис. 2. Графік залежності функції $\Phi(z)$ від інтенсивності λ_2

Із [6] відомо, що сума значень будь-якої дробово-раціональної функції:

$f(z)=\frac{d_m z^m+d_{m-1}z^{m-1}+\ldots d_1 z+d_0}{\ell_m z^m+\ell_{m-1}z^{m-1}+\ldots+\ell_1 z+\ell_0}$, $d_m\neq 0, \ell_m\neq 0$,

що досліджується при значеннях комплексних пов'язаних аргументів, може бути представлена у вигляді: $\frac{(\tau+i\beta)}{(\gamma+i\beta)}+\frac{(\tau-i\theta)}{(\gamma-i\theta)}$, де τ,β,γ,θ – деякі коефіцієнти.

Використавши вираз Ейлера [6], отримаємо:

$$\phi(x)=\sum_{k=1}^{6}\operatorname{Res}_{z=z_k}\left(e^{zx}\Phi(z)\right)=$$

$$e^{(a+\delta i)x}\frac{\tau+i\beta}{\gamma+i\theta}+e^{(a-\delta i)x}\frac{\tau-i\beta}{\gamma-i\theta}= \quad (10)$$

$$\frac{2e^{ax}}{\gamma^2+\theta^2}\left((\tau\gamma+\beta\theta)\cos(\delta x)+(\tau\gamma-\beta\theta)\sin(\delta x)\right),$$

де $\tau=a^3u-3a\delta^2u+a^2v-\delta^2v+ab+k$, $\beta=3a^2\delta u-\delta^3u+2a\delta v+\delta b$,

$$\gamma=7a^6-10a^4\delta^2+105a^2\delta^4-7\delta^6+6g_6a^5-$$
$$60g_6a^3\delta^2+30g_6a\delta^4+5g_5a^4-30g_5a^2\delta^2+5g_5\delta^4+$$
$$4g_4a^3-12g_4a\delta^2+3g_3a^2-3g_3\delta^2+2g_2a+g_1,$$
$$\theta=49a^5\delta-140a^3\delta^3+49a\delta^5+30g_6a^4\delta-60g_6a^2\delta^3+$$
$$6g_6\delta^5+20g_5a^3\delta-20g_5a\delta^3+12g_4a^3\delta-4g_4\delta^3+6g_3a\delta+2g_2\delta.$$

На рис. 3 представлені криві щільності розподілу $\varphi(x)$ ймовірностей часу виконання алгоритму визначення комплексу DOM XSS вразливостей для приведених вище умов (у якості вхідних даних використовувалися корені поліному (8). При цьому рис. 3 а відповідає випадку, коли в якості вхідних даних $(a+\delta i)$ використовувалося значення *x7*. Рис. 3 б відповідає випадку, коли в якості вхідних даних використовувалося значення *x1,* рис. 3 в – *x3,* рис. 3 г – *x4,* рис. 3 д – *x5,* рис. 3 е – *x6*.

Зовнішній вигляд кривих графіків рис. 3 дає підстави припустити, що не всі знайдені вище рішення (коріння полінома (8)) застосовні при математичному та імітаційному моделюванні в якості вхідних даних. Так значення *x1, x6* і *x7* неможливо надалі використовувати при аналізі і моделюванні. У той же час зовнішній вигляд графіків, отриманих для значень *x3* і *x5* дає підстави припустити, що випадкова величина часу виконання алгоритму аналізу DOM XSS уразливості має гамма-розподіл.

Перевіримо цю гіпотезу за критерієм χ^2 Пірсона [6, 8-9]: $\chi^2=N^*\sum_{i=1}^{k}(P_i^*-P_i)^2/P_i$, де k – число розрядів (інтервалів) статистичного ряду; P_i^* і P_i – «статистична» та теоретична ймовірність події.

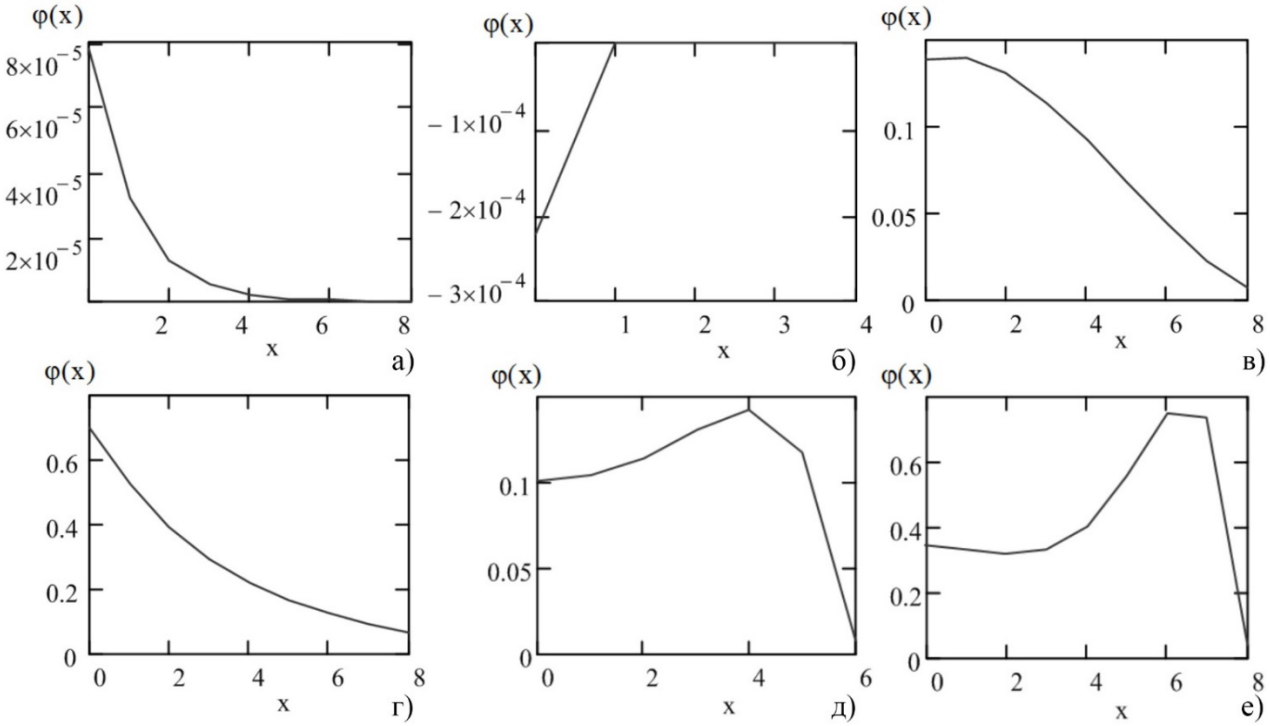

Рис. 3. Графік щільності розподілу $\varphi(x)$ ймовірності часу виконання алгоритму аналізу DOM XSS вразливості

В результаті експерименту були отримані теоретичні значення χ^2 і табличне значення $\overline{\chi^2}$, протилежне правобічній ймовірності розподілу χ^2.

Проведена перевірка показала, що висунуту гіпотезу можна вважати правдоподібною або, принаймні, не суперечить отриманим при математичному моделюванні результатами. Це підтверджується тим, що при досить великому значенні довірчої ймовірності $Q = 0{,}95$ для всіх розглянутих *x2* і *x5* відповідні значення χ^2 ($\chi_1^2 = 19{,}3$, $\chi_2^2 = 15{,}1$) $<< \overline{\chi^2} = 101{,}9$ дозволяють визнати розбіжності між «статистичними» (P_i^*) і теоретичними (P_i) можливостями настання події несуттєвою.

МАТЕМАТИЧНА МОДЕЛЬ ТЕХНОЛОГІЇ ТЕСТУВАННЯ УРАЗЛИВОСТІ ДО SQL ІН'ЄКЦІЙ. Проведені дослідження [2-5, 6] показали, що на основі аналізу методології тестування уразливості Web-додатків до DOM XSS і матеріалів Open Web Application Security Project [7-9], можна розробити алгоритм аналізу уразливості Web-додатків до SQL ін'єкцій. Відмінною особливістю даного алгоритму є облік тільки уразливості, яка є в GET параметрах URL і використовує тільки сліпий метод ін'єкції SQL коду, що використовує особливість використання булевих операторів в SQL запитах (Boolean blind SQL injection) [6-9].

Етапи алгоритму можна описати таким чином:

1. З введеного URL посилання виходить список GET параметрів.

2. Виконується перевірка стабільності Web-сторінки. Для цього виконується два послідовних запити в Web-сторінки і обчислюється відстань між вмістом HTML коду сторінки за допомогою критерію Джаро-Вінклера [9]. Якщо значення критерію менше певного порогового значення, виконувати подальший аналіз неможливо.

3. У параметр GET запиту виконується ін'єкція SQL коду, який не змінює результат запиту до бази даних і зберігається результуючий HTML код.

4. У параметрі GET запиту виконується ін'єкція SQL коду, який змінює результат запиту до бази даних, призводить або до отримання повного набору даних з таблиці, або до відсутності результату, після чого зберігається результуючий HTML код.

5. За допомогою критерію Джаро-Вінклера виконується порівняння результатів ін'єкції SQL коду. Якщо значення критерію менше певного порогового значення, то в даному GET параметрі є можлива вразливість до SQL ін'єкції.

6. Кроки 2 - 5 повторюються для всіх параметрів GET запиту наданого URL.

На підставі поданого алгоритму розробимо GERT-модель технології тестування уразливості до SQL ін'єкцій.

Побудуємо, відповідно до представленого описом мережеву GERT-модель технології тестування уразливості до SQL ін'єкцій. Графічне зображення GERT-моделі представлено на рис. 4.

У представленій мережі вузли графа інтерпретуються станами комп'ютерної системи в процесі тестування уразливості до SQL ін'єкцій, а гілки графа – ймовірносно-тимчасовими характеристиками переходів між станами. Зокрема гілка (1, 2) характеризує час отримання і аналізу GET-параметрів з введеного URL посилання. Гілка (2, 3) відображає час відправлення первинних і вторинних запитів в Web-сторінки. Гілка (3, 4) задає випадковий час порівняння сторінок (час обчислення відстані між вмістом HTML коду сторінки за допомогою критерію Джаро-Вінклера). Гілка (4, 5) характеризує час, за яке виконується ін'єкція SQL коду, який не змінює результат запиту до бази даних, а також який змінює результат запиту до бази даних відповідно. Далі гілка (5, 6) характеризує час порівняння результатів ін'єкції SQL коду. Гілка (4, 2) характеризує тимчасові характеристики повернення системи в початковий стан, коли значення критерію Джаро-Вінклера менше певного порогового значення, в той же час гілка (6, 2) відображає тимчасові характеристики переходу до нової перевірки в разі якщо значення критерію Джаро-Вінклера більше певного порогового значення.

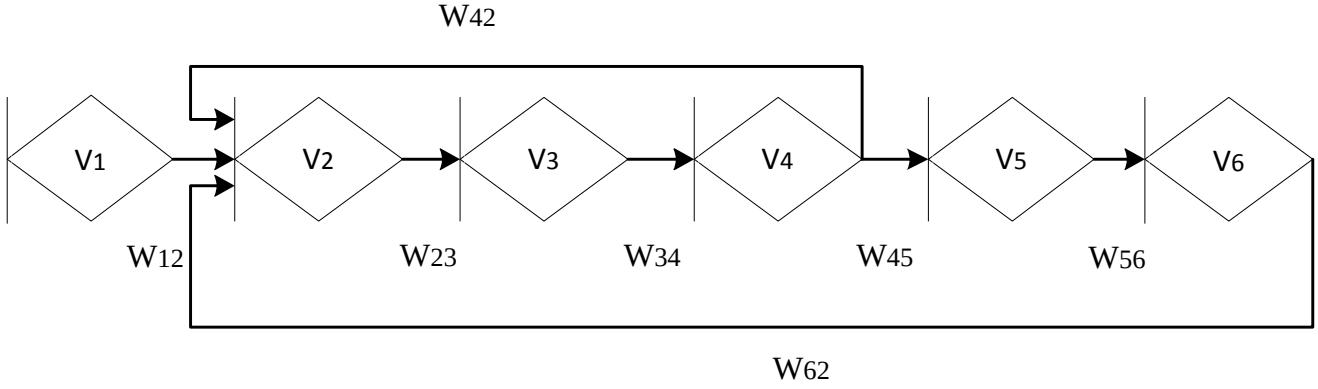

Рис. 4. GERT-модель технології тестування вразливості до SQL ін'єкцій

Як зазначено вище щільність розподілу ймовірностей часу виконання технології тестування уразливості до SQL ін'єкцій дорівнює:

$$\varphi(x)=\frac{1}{2\pi i}\int_{-i\infty}^{i\infty} e^{zx}\frac{vz^2+bz+k}{\left(z^7+rz^6+cz^5+dz^4+gz^3+hz^2+wz+m\right)}dz, \quad (13)$$

де операції інтегрування виконується за допомогою інтеграла Бромвича-Вагнера [6].

Тоді вираз $e^{zx}\Phi(z)$ можна представити у вигляді:

$$e^{zx}\Phi(z)=\frac{e^{zx}\left(vz^2+bz+k\right)}{z^7+rz^6+cz^5+dz^4+gz^3+hz^2+wz+m}=\frac{\mu(z)}{\psi(z)}. \quad (14)$$

Тоді щільність розподілу часу виконання алгоритму тестування вразливості до SQL ін'єкціям дорівнює:

$$\phi(x)=\sum_{k=1}^{7}\mathrm{Re}\,s\left[e^{zx}\Phi(z)\right]=\sum_{k=1}^{7}\frac{\mu(z_k)}{\psi(z_k)}=\sum_{k=1}^{7}\frac{e^{zx}\left(vz^2+bz+k\right)}{7z_k^6+6rz_k^5+5cz_k^4+4dz_k^3+3gz_k^2+2hz_k+w}. \quad (15)$$

Багаточлен $rz^6+cz^5+dz^4+gz^3+hz^2+wz+m$ породжує сім полюсів. Рішення рівняння

$$rz^6+cz^5+dz^4+gz^3+hz^2+wz+m=0. \quad (16)$$

Може бути знайдено будь-яким методом, наприклад, по формулам Вієта [6]. В результаті обчислюється особливі точки $z_1, z_2, z_3, z_4, z_5, z_6, z_7$.

Таким чином, на основі експоненційної GERT-мережі розроблено математичну модель технології тестування уразливості до SQL ін'єкцій, яка відрізняється від відомих, вдосконаленим способом визначення відстані між результатами ін'єкції. Використання в запропонованому способі критерію Джаро-Вінклера, для порівняння результатів ін'єкції SQL коду і введення порогового значення дозволить підвищити точність результатів тестування уразливості до SQL ін'єкцій.

Дослідження GERT-моделі технології тестування уразливості до SQL ін'єкцій. Розглянемо приклад атаки SQL ін'єкцій. Суть таких ін'єкцій - впровадження в дані (передані через GET, POST запити або значення Cookie) довільного SQL коду.

Знайдемо щільності розподілу φ(x) ймовірностей часу виконання алгоритму при умові, що z обираються як корені рівняння $(z^7+rz^6+cz^5+dz^4+gz^3+hz^2+wz+m)=0$, умовні ймовірності та інтенсивності в гілках *GERT*-мережі мають значення:

$p_1 = p_2 = p_3 = p_4 = p_5 = 0,999999$, $p_6 = 0,9$, $\lambda_1 =$, $\lambda_2 = \lambda_3 = 0,9999$ $\lambda_4 = 0,8$, $\lambda_5 = 0,1$, $\lambda_6 = 0,999999$.

З урахуванням наведених ознак GERT-мережі, відповідно до виразу (12), а також використовуючи спеціалізований математичний пакет Mathcad, отримаємо, що в знаменнику вираз (13) сформований поліном

$$x^7 - 0,1x^6 - 4,174x^5 + 2,471x^4 - 4,509x^3 + 4,128x^2 + 2,014x - 0,169 = 0. \quad (17)$$

Корені цього полінома (та відповідно функція $\Phi(z)$) дорівнюють:

x1 $\approx -2,11254039866286$, *(P(x1)* ≈ 0*;iter = 1);*

x2 $\approx -0,561885634027132$, *(P(x2)* ≈ 0*; iter = 4);*

x3 $\approx -0,208185977139001 - i \cdot 0,60944124336833$, *(P(x3)* ≈ 0*; iter = 5);*

x4 $\approx -0,208185883644938 + i \cdot 0,609441306673327$, *(P(x4)* ≈ 0*; iter = 4);*

x5 $\approx -0,103581224605665$, *(P(x5)* ≈ 0*; iter = 3);*

x6 $\approx 1,64718955898524 - i \cdot 0,775107663208$, *(P(x6)* ≈ 0*; iter = 1);*

x7 $\approx 1,64718955909435 + i \cdot 0,775107667929698$, *(P(x7)* ≈ 0*; iter = 4).*

Дослідимо залежність функції $\Phi(z)$ від інтенсивності z.

На рис. 5 представлена крива графіка залежності функції $\Phi(z)$ від z в розглянутих вище умовах. Як видно з малюнка випадкова величина z розподілена відповідно до показникового закону.

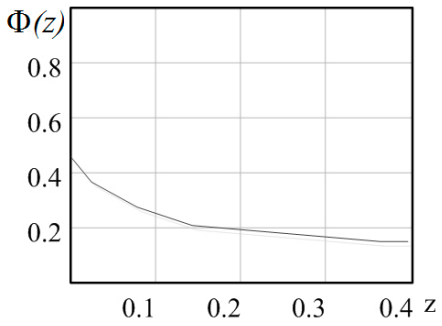

Рис. 5. Графік залежності функції $\Phi(z)$ від інтенсивності z

Аналогічно алгоритму розрахунку $\varphi(x)$, який використовувався вище, знайдемо цю функцію та дослідимо її з використанням математичного пакету *Mathcad*. У відповідності до формули (15) $\varphi(x)$ дорівнює:

$$\phi(x) = \sum_{k=1}^{6} \operatorname{Res}_{z=z_k} \left[e^{zx} \Phi(z) \right] = \frac{e^{(a+\delta i)x} \left(v(a+\delta i)^2 + b(a+\delta i) + k \right)}{\left(7u(a+\delta i)^6 + 6r(a+\delta i)^5 + 5c(a+\delta i)^4 + 4d(a+\delta i)^3 + 3g(a+\delta i)^2 + 2h(a+\delta i) + w \right)} - \frac{e^{(a-bi)x} \left(v(a-\delta i)^2 + b(a-\delta i) + k \right)}{\left(7u(a-\delta i)^6 + 6r(a-\delta i)^5 + 5c(a-\delta i)^4 + 4d(a-\delta i)^3 + 3g(a-\delta i)^2 + 2h(a-\delta i) + w \right)}. \quad (18)$$

Аналогічно підходу, який використовувався вище, використовуючи вираз Ейлера [6], отримаємо:

$$\phi(x) = \sum_{k=1}^{6} \operatorname{Res}_{z=z_k} \left(e^{zx} \Phi(z) \right) = e^{(a+\delta i)x} \frac{\tau + i\beta}{\gamma + i\theta} + e^{(a-\delta i)x} \frac{\tau - i\beta}{\gamma - i\theta} = \frac{2e^{ax}}{\gamma^2 + \theta^2} \left((\tau\gamma + \beta\theta)\cos(\delta x) + (\tau\gamma - \beta\theta)\sin(\delta x) \right), \quad (19)$$

де $\tau = a^2 v - \delta^2 v + ab + k$, $\beta = 2a\delta v - \delta b$, $\gamma = 7ua^6 - 10ua^4\delta^2 + 105ua^2\delta^4 - 7u\delta^6 + 6ra^5 - 60ra^3\delta^2 + 30ra\delta^4 + 5ca^4 - 30ca^2\delta^2 + 5c\delta^4 + 4da^3 - 12da\delta^2 + 3ga^2 - 3g\delta^2 + 2ha + w$, $\theta = 49ua^5\delta - 140ua^3\delta^3 + 49ua\delta^5 + 30ra^4\delta - 60ra^2\delta^3 + 6r\delta^5 + 20ca^3\delta - 20ca\delta^3 + 12da^3\delta - 4d\delta^3 + 6ga\delta + 2h\delta$.

На рис. 6 представлені криві щільності розподілу $\varphi(x)$ ймовірностей часу виконання технології тестування вразливості до SQL ін'єкцій для наведених вище умов в якості вхідних даних $(a + \delta i)$ використовувалися корені полінома (17)).

При цьому рис. 6а відповідає випадку коли в якості вхідних даних використовувалося значення – *x1*, рис. 6б – *x2*, рис. 6в – *x3*, рис. 6г – *x4*, рис. 6д – *x5*, рис. 6е – *x6*, рис. 6ж – *x7*.

Як і в розглянутому вище прикладі, зовнішній вигляд кривих графіків рис. 6 дає підстави припустити, що не всі знайдені вище рішення (корені полінома (17)) застосовні при математичному та імітаційному моделюванні в якості вхідних даних.

Тож значення *x3, x4, x6* і *x7* неможливо надалі використовувати при аналізі і моделюванні. У той же час зовнішній вигляд графіків, отриманих для значень *x1, x2 і x5* дає підстави припустити, що

випадкова величина часу виконання технології тестування вразливості до SQL ін'єкцій відповідає гамма-розподілу (близьке до експоненціального).

Результати перевірки цієї гіпотези за критерієм χ^2 Пірсона [6] підтвердили її правдоподібність. Так при досить великому значенні довірчої ймовірності $Q = 0{,}95$ для всіх розглянутих *x1, x2* і *x5* відповідні значення χ^2 ($\chi_1^2 = 19{,}3$, $\chi_2^2 = 15{,}1$, $\chi_5^2 = 25{,}6$) $<< \overline{\chi^2} = 101{,}9$.

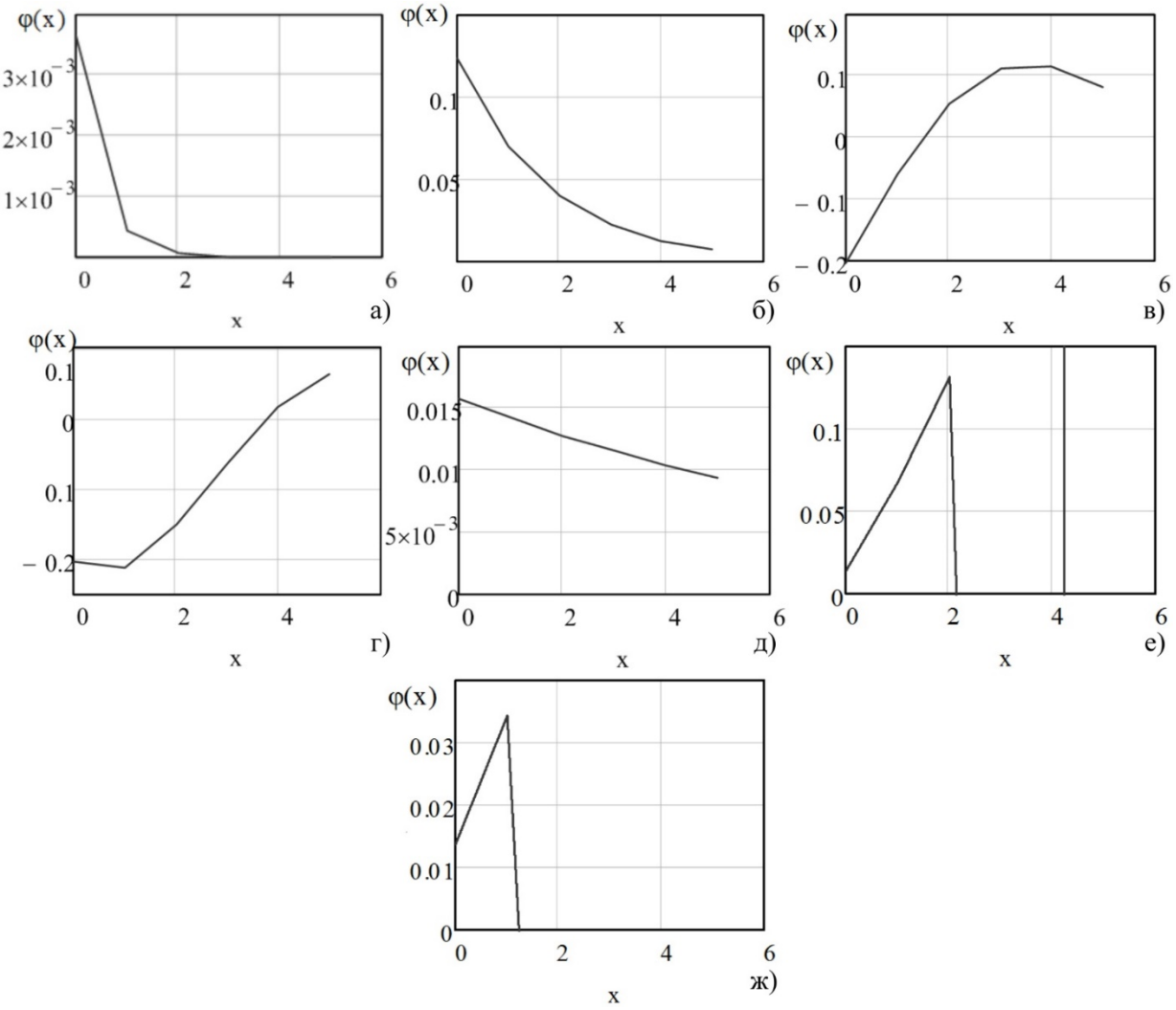

Рис. 6. Графіки щільності розподілу φ(x) ймовірності часу виконання технології тестування вразливості до SQL ін'єкцій

ВИСНОВКИ

В роботі розроблений комплекс математичних моделей технології тестування WEB-додатків. В основу математичного моделювання покладено підхід GERT-мережевого синтезу. В результаті розроблено математичні моделі технології тестування DOM XSS уразливості і технології тестування уразливості до SQL ін'єкцій.

Математична модель технології тестування DOM XSS уразливості відрізняється від відомих, урахуванням виконання або аналізу DOM структури, що дає можливість провести аналітичну оцінку тимчасових витрат тестування зазначеної уразливості в умовах реалізації стратегії розробки безпечного програмного забезпечення. Математична модель технології тестування уразливості до SQL ін'єкцій відрізняється від відомих, вдосконаленим способом визначення відстані між результатами ін'єкції. Використання в запропонованому способі критерію Джаро-Вінклера, для порівняння результатів ін'єкції SQL коду і введення порогового значення дозволить підвищити точність результатів тестування безпеки програмного забезпечення.

В ході дослідження представлених моделей було визначено, що випадкова величина часу виконання розглянутих технологій тестування в цілому відповідає гамма-розподілу. Перевірка цієї гіпотези проведена за критерієм χ^2 Пірсона.

ЛІТЕРАТУРА

[1]. В. Ковалев, ГЕРТ-сетевой анализ мультеверсионных архитектур программного обеспечения. Успехи современного естествознания, №9, С. 161-164, 2011.

[2]. А. Коваленко, А. Смирнов, Н. Якименко, А. Доренский, "Проблемы анализа и оценки рисков информационной деятельности", *Системи обробки інформації,* № 3(140), С. 40-42, 2016.

[3]. А. Коваленко, А. Смирнов, "Методы качественного анализа и количественной оценки рисков разработки программного обеспечения", *Системи обробки інформації*, № 5(142), С. 153-157, 2016.

[4]. А. Коваленко, А. Смирнов, "Использование псевдобулевых методов бивалентного программирования для управления рисками разработки программного обеспечения", *Системи управління, навігації та зв'язку,* № 1 (37), С. 98-103, 2016.

[5]. А. Коваленко, "Метод управления рисками разработки программного обеспечения", *Системи управління, навігації та зв'язку*, № 2 (38), С. 93-100, 2016.

[6]. В. Липаев, *Надежность и функциональная безопасность комплексов программ реального времени,* 2013, 176 с.

[7]. С. Семенов, Г. Швачич, Т. Карпова, В. Волнянський, "Застосування багатопроцесорних систем для удосконалення технологічних процесів", *Системи обробки інформації*, № 3(140), С. 221-226, 2016.

[8]. Spring Framework. [Electronic resource]. Online: http://projects.spring.io/spring-framework.

[9]. Fowler M. Inversion of Control Containers and the Dependency Injection pattern. Electronic resource]. Online: https://martinfowler.com/articles/injection.html.

GERT-СЕТЕВОЙ СИНТЕЗ ТЕХНОЛОГИИ ТЕСТИРОВАНИЯ УЯЗВИМОСТИ WEB-ПРИЛОЖЕНИЙ

В работе представлены результаты исследования и алгоритмы тестирования на уязвимость к одним из наиболее распространенных видов атак на Web-приложения – DOM XSS и SQL инъекции. Аргументировано выбран подход математического моделирования на основе GERT-сетей. Разработан комплекс математических моделей технологии тестирования Web-приложений. В основу математического моделирования положен подход GERT-сетевого синтеза. В результате разработаны математические модели технологии тестирования DOM XSS уязвимости и технологии тестирования уязвимости к SQL инъекциям. Математическая модель технологии тестирования DOM XSS уязвимости отличается от известных, учетом выполнения или анализа DOM структуры. Математическая модель технологии тестирования уязвимости к SQL инъекциям отличается от известных, усовершенствованным способом определения расстояния между результатами инъекции.

Ключевые слова: атаки на Web-приложения, DOM XSS, SQL инъекции, GERT-сети.

GERT-NETWORK SYNTHESIS OF VULNERABILITY TESTING TECHNOLOGY OF WEB-APPLICATIONS

The paper presents research results and vulnerability testing algorithms for one of the most common types of attacks on Web applications - DOM XSS and SQL injection. The approach of mathematical modeling based on GERT-networks is argued. A set of mathematical models of Web application testing technology has been developed. The basis of mathematical modeling is the approach of GERT-network synthesis. As a result, mathematical models of DOM XSS testing technology and vulnerability testing technology for SQL injections have been developed. The mathematical model of the DOM XSS testing technology vulnerability differs from the known, taking into account the execution or analysis of the DOM structure. The mathematical model of vulnerability testing technology for SQL injections differs from the known ones by an improved method of determining the distance between the results of injection.

Keywords: attacks on Web-applications, DOM XSS, SQL injections, GERT-networks.

Коваленко Олександр Володимирович, к.т.н., доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, Кропивницький, Україна.
E-mail: clashav@gmail.com.

Коваленко Александр Владимирович, к.т.н., доцент кафедры кибербезопасности и программного обеспечения Центральноукраинского национального технического университета, Кропивницкий, Украина.

Kovalenko Oleksandr, Candidate of Engineering Sciences, Associate Professor of Cybersecurity & Software Academic Department, Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine.