Methods of information systems protection

УДК 004.056 **doi: 10.20998/2522-9052.2020.3.17**

Р. В. Киричок, Г. В. Шуклін, О. В. Барабаш, Г. І. Гайдур

Державний університет телекомунікацій, Київ, Україна

МОДЕЛЮВАННЯ МЕХАНІЗМУ ВАЛІДАЦІЇ ВРАЗЛИВОСТЕЙ ПРИ АКТИВНОМУ АНАЛІЗІ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ МЕРЕЖ ЗА ДОПОМОГОЮ ПОЛІНОМІВ БЕРНШТЕЙНА

Анотація. Предметом вивчення у статті є модель процесу активного аналізу захищеності інформаційних систем та мереж, зокрема одного з її ключових компонентів, а саме механізму валідації вразливостей. **Метою дослідження** є розробка математичної моделі аналізу кількості успішної та негативної валідацій за час раціонального циклу валідації виявлених вразливостей під час автоматизованого активного аналізу захищеності корпоративної мережі. **Результати:** на основі проведених в роботі спостережень та досліджень функціонування засобів експлуатації виявлених вразливостей було прийнято рішення щодо опису динаміки процесів валідації саме за допомогою поліномів Бернштейна, які успішно апроксимують аналітичні залежності для кількісних характеристик процесу валідації вразливостей. При цьому, на основі порівняння емпіричних та розрахункових значень даних характеристик встановлено, що відхилення є допустимими. **Висновки:** розроблена математична модель забезпечує отримання аналітичних залежностей для кількості успішно валідованих, невалідованих вразливостей та кількості випадків валідації вразливостей, що призвели до критичних помилок за час раціонального циклу валідації виявлених вразливостей.

Ключові слова: активний аналіз захищеності; валідація вразливостей; корпоративна мережа; поліноми Бернштейна.

Вступ

За останні роки, разом зі зростанням поширеності корпоративних мереж та ефективності їх використання для створення єдиної гнучкої інформаційної системи будь-якої великої організації, питання забезпечення інформаційної безпеки (ІБ) таких мереж набуває надзвичайно великого значення.

При цьому, одним із актуальних напрямків забезпечення ІБ корпоративних мереж є впровадження не лише детектуючих механізмів кіберзахисту, які несуть завідомо запізнілий характер реагування, але й превентивних методів та засобів забезпечення ІБ. Серед числа останніх, найперспективнішими залишаються системи активного аналізу захищеності (САА3), які дозволяють не лише виявляти вразливості, але й валідувати їх, тобто підтверджувати можливість реалізації конкретних вразливостей за рахунок їх експлуатації, тим самим встановлюючи фактичний стан захищеності інформаційних систем та мереж, а також формувати рекомендації щодо усунення підтверджених вразливостей.

Постановка проблеми. Існуючі САА3 базуються на практичному аудиті інформаційної безпеки, включаючи пасивні та активні методи виявлення і підтвердження вразливостей інформаційних систем (зокрема, методи проведення тестування на проникнення). При цьому, провідні дослідження та розробки передбачають використання механізмів штучного інтелекту, таких як, класичні алгоритми машинного навчання, нейронні мережі, марківські процеси прийняття рішень в частково спостережуваному середовищі та інші, для прогнозування, планування та генерування успішного вектора атаки, автоматизації процесу пошуку та експлуатації вразливостей. Однак, слід зазначити, що при розробці подібних методів мало приділяється уваги дослідженню одного з ключових компонентів будь-якої САА3, а саме механізму валідації вразливостей, зокрема його аналізу та моделюванню.

Аналіз останніх досліджень і публікацій. Проведений аналіз останніх досліджень і публікацій показав, що існує ряд моделей та алгоритмів, які дозволяють з різним ступенем деталізації описати процес активного аналізу захищеності, зокрема через моделювання мережевих атак. Дані моделі використовують різну математичну базу, однак більшість з них засновані на кінцевих автоматах і представляють процес аналізу захищеності або атаку в якості послідовності станів автомата.

Основним недоліком використання моделей графів атак в аналізі захищеності є можливість їхнього застосування лише для сценаріїв проведення аналізу захищеності в невеликих мережах, через проблему швидкого зростання станів. Для вирішення цієї проблеми, у роботі [1] було трансформовано сценарій проникнення в подання PDDL (Planning Domain Definition Language) та використано класичний алгоритм планування для пошуку шляхів атак. Окрім цього, для врахування невизначеності в сценарії тестування на проникнення комп'ютерної мережі, в [2] проблема планування атак була змодельована в термінах частково спостережуваних марківських процесів прийняття рішень (POMDP).

Однак, оскільки підходи, засновані на POMDP, не дозволяють масштабувати модель до прийнятних розмірів, в роботі [3], автори моделюють тестування на проникнення як частково спостережувану умовну проблему, допускаючи часткову спостережуваність та недетерміновані ефекти дії.

Також, слід відзначити роботу [4], в якій було обговорено розроблення експертної системи на основі POMDP та запропоновано поліпшення її ефективності за рахунок використання методології авто-

матизованого планування та процесу прийняття рішень Маркова.

З точки зору обмеження ресурсів та обчислювальної складності алгоритмів планування атак, яка може виникнути через складність планування графів атак, необхідно відмітити роботи [5-7]. Зокрема в [5] було запропоновано автоматичний алгоритм генерування графа атак при тестуванні на проникнення, який скорочує надлишкову інформацію шляхом оптимізації топології мережі перед створенням самого графа атак.

Таким чином, з короткого літературного огляду можна заначити, що при моделюванні процесу активного аналізу захищеності, зокрема тестування на проникнення, зовсім не розглядається питання якості процесу такого аналізу.

Метою статті є розробка математичної моделі аналізу кількості успішної та негативної валідацій за час раціонального циклу валідації виявлених вразливостей під час автоматизованого активного аналізу захищеності корпоративної мережі.

Виклад основного матеріалу

Як вже зазначалося раніше, існуючі системи активного аналізу захищеності інформаційних систем та мереж включають два типи засобів: пасивні – засоби виявлення потенційних вразливостей цільових систем (так звані сканери безпеки, серед яких слід виділити NeXpose, Nessus vulnerability scanner, OpenVAS Vulnerability Scanner) та активні – засоби експлуатації виявлених вразливостей, або як їх ще називають – засоби проведення тестування на проникнення (Metasploit Framework, Core Impact, SAINT Security Suite та ін.).

Загалом, необхідність в перевірці можливості реалізації виявлених вразливостей, тобто їх валідації, виникає через те, що сканери безпеки дозволяють виявляти лише потенційні вразливості цільових систем, при цьому допускаючи хибність таких спрацювань, яка полягає в неможливості фактичної реалізації виявленої вразливості з боку зловмисника.

І тому в роботі було проведено ряд спостережень функціонування саме засобів експлуатації виявлених вразливостей на основі яких встановлено, що якість валідації вразливостей хостів цільової корпоративної мережі визначається вектором $\left(q_s, q_f, q_c\right)$ трьохвимірного векторного простору, де q_s – абсциса, яка визначає кількість успішно валідованих вразливостей, q_f – ордината, яка визначає кількість невалідованих вразливостей та q_c – апліката, яка визначає кількість випадків валідації вразливостей, що призвели до критичних помилок на цільовому хості та подальшої втрати з ним зв'язку.

Кожна з вказаних координат з однієї сторони неперервно змінюється в часі (час раціонального циклу), протягом якого проводиться активний аналіз захищеності окремого цільового хоста та корпоративної мережі в цілому, а з іншої, всі три координати пов'язані між собою деякою функціональною залежністю.

Однак, на відміну від детермінованих динамічних систем, які можна описати системами диференціальних рівнянь, що будуються на основі природи системи, завдання виявлення валідації вразливостей не є однозначним. Тому, варто розв'язувати дане завдання, створюючи аналітичні залежності, які в свою чергу є розв'язками деякої системи диференціальних рівнянь.

Для цього, спершу було проведено дослідження роботи одного з відомих засобів автоматизації процесу активного аналізу захищеності – Armitage [8]. Даний засіб є безкоштовним графічним інструментом управління кібератаками з відкритим кодом, фактично графічною оболонкою для раніше згадуваного засобу експлуатації вразливостей Metasploit framework, яка спрощує та в певній мірі автоматизує роботу з фреймворком.

Дослідження відбувалося за рахунок симуляції процесу валідації вразливостей окремих хостів потенційної цільової корпоративної мережі на спеціально створеному тестовому стенді, результати наведені в табл. 1 (де J – загальна кількість спроб експлуатації виявлених вразливостей окремого хоста цільової корпоративної мережі; t – загальний час проведення валідації виявлених вразливостей окремого хоста цільової корпоративної мережі, виражений в секундах).

При цьому, список хостів було сформовано виходячи з статистичних даних щодо розповсюдженості використання конкретних операційних систем в світі [9] та зокрема в Україні [10].

Таблиця 1 – **Результати проведення валідації вразливостей за допомогою armitage**

Платформа (ОС)	J	q_s	q_f	q_c	t
Windows XP SP2	312	3	306	3	345
Windows XP SP3	98	3	93	2	86
Windows 7	85	2	80	3	65
Windows 8.1	83	1	81	1	58
Windows 10	84	0	83	1	154
Windows Server 2008 R2	96	2	92	2	82
Windows Server 2016	39	0	39	0	71
Mac OS X 10.13	63	1	61	1	115
Mac OS X 10.14	46	1	45	0	83
Metasploitable 2	765	3	762	0	293
Metasploitable 3	780	3	777	0	330

З даних таблиці видно, що час раціонального циклу проведення валідації вразливостей, в даному випадку, складає 345 секунд. Здійснивши нормування відрізка часу $[0;345]$, отримуємо нормований час на відрізку $[0;1]$, який представлено в табл. 2. Тоді значення змінних $q_s(t_н)$, $q_f(t_н)$, $q_c(t_н)$, як функції від часу нормування, представлені в табл. 3.

Таблиця 2 – **Нормування часу раціонального циклу**

t – реальний час	0	58	65	71	82	83	86	115	154	293	330	345	0
$t_н$ – нормований час	0	0,168	0,188	0,206	0,238	0,241	0,249	0,333	0,446	0,849	0,957	1	0

Таблиця 3 – **Значення кількості успішно валідованих $q_s(t_н)$, невалідованих вразливостей та випадків валідацій $q_f(t_н)$, що призвели до критичних помилок $q_c(t_н)$**

$t_н$ – нормований час	0	0,168	0,188	0,206	0,238	0,241	0,249	0,333	0,446	0,849	0,957	1	0
$q_s(t_н)$	0	1	2	0	2	1	3	1	0	3	3	3	0
$q_f(t_н)$	0	81	80	39	92	45	93	61	83	762	777	306	0
$q_c(t_н)$	0	1	3	0	2	0	2	1	1	0	0	3	0

Використовуючи теорему Бернштейна [11], сутність якої полягає в тому, що довільну неперервну функцію $f(t)$, яка визначена і неперервно-диференційована на відрізку $[0;1]$, можна представити у вигляді поліному

$$f(t_н) = \sum_{k=0}^{n} f\left(k/n\right) b_{k,n}(t_н), \qquad (1)$$

де $b_{k,n}(t_н) = C_n^k t_н^{\,k} (1-t_н)^{n-k}$.

Використовуючи дані з табл. 3 і представлення (1) були отримані початкові аналітичні залежності для кількості успішно валідованих вразливостей $q_S = q_S(t_н)$

$$\begin{aligned} q_S(t_н) = {} & q_S(0) b_{0.11}(t_н) + q_S(0{,}168) b_{1.11}(t_н) + \\ & + q_S(0{,}188) b_{2.11}(t_н) + q_S(0{,}206) b_{3.11}(t_н) + \\ & + q_S(0{,}238) b_{4.11}(t_н) + q_S(0{,}241) b_{5.11}(t_н) + \\ & + q_S(0{,}249) b_{6.11}(t_н) + q_S(0{,}333) b_{7.11}(t_н) + \\ & + q_S(0{,}446) b_{8.11}(t_н) + q_S(0{,}849) b_{9.11}(t_н) + \\ & + q_S(0{,}957) b_{10.11}(t_н) + q_S(1) b_{11.11}(t_н). \end{aligned}$$

Після підстановки відповідних значень з табл. 3:

$$\begin{aligned} q_S(t_н) = {} & b_{1.11}(t_н) + 2b_{2.11}(t_н) + 2b_{4.11}(t_н) + \\ & + b_{5.11}(t_н) + 3b_{6.11}(t_н) + b_{7.11}(t_н) + \\ & + 3b_{9.11}(t_н) + 3b_{10.11}(t_н) + 3b_{11.11}(t_н). \end{aligned} \qquad (2)$$

В табл. 4 представлені значення $b_{k,11}(t_н)$ для $k = \overline{0...11}$. В табл. 5 представлені порівняльні значення результатів обчислення і даних з табл. 3 (($t_н$ – нормований час, $q^e{}_s(t_н)$, $q^p{}_s(t_н)$ – емпіричні та розрахункові значення відповідно; $\theta = \left|q_S^e(t_н) - q_S^p(t_н)\right|$ – відхилення). Як видно з табл. 5, відхилення між емпіричними даними і розрахунковими допустимі, а при збільшенні кількість значень, ці відхилення стають все менші і менші.

Однак, для подальших досліджень, пов'язаних з хибними спробами валідації вразливостей та з випадками валідації, які призвели до критичних помилок, ця різниця не суттєва.

Графік залежності (2) представлено на рис. 1. З графіка видно, що функція $q_S = q_S(t_н)$ успішної валідації вразливостей задовольняє умові Ліпшиця [11], тобто, для довільних $t_н^{(1)}, t_н^{(2)} \in [0;1]$ існує $K > 0$, що виконується нерівність

$$\left|q_S(t_н^{(1)}) - q_S(t_н^{(2)})\right| \le K \left|t_н^{(1)} - t_н^{(2)}\right|. \qquad (3)$$

З умови (3) випливає, що існує прямокутна область, за межі якої графік функції $q_S = q_S(t_н)$ не виходить. Це дає можливість в подальшому будувати закони розподілу ймовірностей кількості успішно валідованих вразливостей, що призведе до методики розрахунку ризиків втрат від невалідованих вразливостей, які призводять до критичних помилок. Крім того, як було показано в [11], при виконанні умови (3), справедлива оцінка

$$\left|B_n(q_S, t_н) - q_S(t_н)\right| \le K\sqrt{t_н(1-t_н)/n}. \qquad (4)$$

З графіка видно, що функція $q_S = q_S(t_н)$ успішної валідації вразливостей задовольняє умові Ліпшиця [11], тобто, для довільних $t_н^{(1)}, t_н^{(2)} \in [0;1]$ існує $K > 0$, що виконується нерівність

$$\left|q_S(t_н^{(1)}) - q_S(t_н^{(2)})\right| \le K \left|t_н^{(1)} - t_н^{(2)}\right|. \qquad (3)$$

З умови (3) випливає, що існує прямокутна область, за межі якої графік функції $q_S = q_S(t_н)$ не виходить.

Це дає можливість в подальшому будувати закони розподілу ймовірностей кількості успішно валідованих вразливостей, що призведе до методики розрахунку ризиків втрат від невалідованих вразливостей, які призводять до критичних помилок.

Таблиця 4 – **Значення поліномів $b_{k,11}(t_н)$**

k	$b_{k,11}(t_н)$	k	$b_{k,11}(t_н)$	k	$b_{k,11}(t_н)$	k	$b_{k,11}(t_н)$	k	$b_{k,11}(t_н)$	k	$b_{k,11}(t_н)$
0	$(1-t)^{11}$	3	$165t^3(1-t)^8$	4	$330t^4(1-t)^7$	6	$462t^6(1-t)^5$	8	$165t^8(1-t)^3$	10	$11t^{10}(1-t)$
1	$11t(1-t)^{10}$	2	$55t^2(1-t)^9$	5	$462t^5(1-t)^6$	7	$330t^7(1-t)^4$	9	$55t^9(1-t)^2$	11	t^{11}

Таблиця 5 – **Порівняльні значення для $q_s(t_н)$**

$t_н$	$q^e{}_s(t_н)$	$q^p{}_s(t_н)$	θ	$t_н$	$q^e{}_s(t_н)$	$q^p{}_s(t_н)$	θ
0	0	0	0	0,249	3	1,181262	1,818738
0,168	1	1,065446	0,065446	0,333	1	1,309026	0,309026
0,188	2	1,100162	0,899838	0,446	0	1,494756	1,494756
0,206	0	1,126111	1,126111	0,849	3	2,425641	0,574359
0,238	2	1,167208	0,832792	0,957	3	2,970647	0,029353
0,241	1	1,171013	0,171013	1	3	3	0

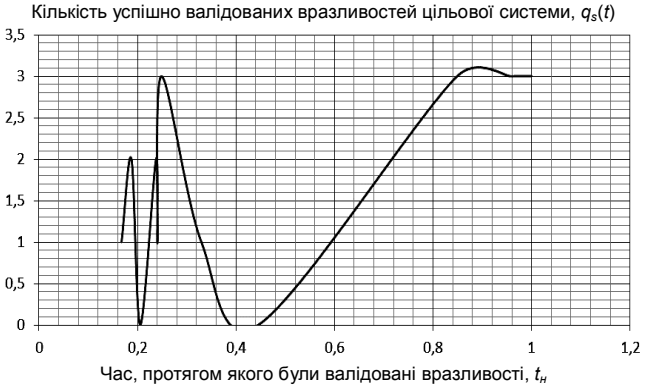

Рис. 1. Залежність кількості успішно валідованих вразливостей цільової системи від часу раціонального циклу

Крім того, як було показано в [11], при виконанні умови (3), справедлива оцінка

$$\left|B_n(q_S,t_н)-q_S(t_н)\right| \le K\sqrt{t_н(1-t_н)/n}\,. \qquad (4)$$

З нерівності (4) випливає, що існує таке додатне число K, при якому

$$\theta = \left|q^e_S(t_н)-q^p_S(t_н)\right| = K\sqrt{t_н(1-t_н)/n}\,. \qquad (5)$$

Залежність (5) дає можливість задавати відповідну точність для визначення степені n полінома Бернштейна. Використовуючи дані з табл. 5 та залежність (5) було отримано максимальне значення K для $q_S = q_S(t_н)$: $\max\left(K_i\right) = 13,949121$, де $i \in [1;11)$.

Аналогічно, використовуючи представлення (1) та дані з табл. 3, отримуємо початкові аналітичні залежності для кількості невалідованих вразливостей $q_f = q_f(t_н)$ (залежність (6), рис. 2) і кількості випадків валідації вразливостей, що призвели до критичних помилок $q_c = q_c(t_н)$ (залежність (7), рис. 3).

$$\begin{aligned} q_f(t_н) &= 81b_{1.11}(t_н)+80b_{2.11}(t_н)+39b_{3.11}(t_н)+\\ &+92b_{4.11}(t_н)+45b_{5.11}(t_н)+93b_{6.11}(t_н)+\\ &+61b_{7.11}(t_н)+83b_{8.11}(t_н)+762b_{9.11}(t_н)+\\ &+777b_{10.11}(t_н)+306b_{11.11}(t_н). \end{aligned} \qquad (6)$$

$$\begin{aligned} q_c(t_н) &= b_{1.11}(t_н)+3b_{2.11}(t_н)+2b_{4.11}(t_н)+\\ &+2b_{6.11}(t_н)+b_{7.11}(t_н)+b_{8.11}(t_н)+3b_{11.11}(t_н). \end{aligned} \qquad (7)$$

В табл. 6 ($q^e{}_f(t_н)$, $q^p{}_f(t_н)$ – емпіричні та розрахункові значення відповідно; $\theta = \left|q^e_f(t_н)-q^p_f(t_н)\right|$ – відхилення) та табл. 7 ($\theta = \left|q^e_c(t_н)-q^p_c(t_н)\right|$ – відхилення; $q^e{}_c(t_н)$, $q^p{}_c(t_н)$ – емпіричні та розрахункові значення відповідно) представлені відповідні порівняльні значення результатів обчислення і даних з табл. 3. Також, слід відзначити, з рис. 2 та 3 видно, що функції $q_f = q_f(t_н)$ і $q_c = q_c(t_н)$ також задовольняють умові Ліпшиця.

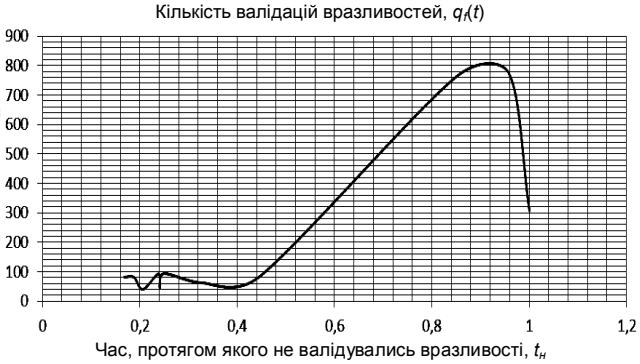

Рис. 2. Залежність кількості невалідованих вразливостей цільової системи від часу раціонального циклу

Рис. 3. Залежність кількості валідацій вразливостей, які призвели до критичних помилок в цільовій системі від часу раціонального циклу

Окрім цього, використовуючи дані з табл. 6 і 7 та залежність (5), отримуємо максимальні значення K $i \in [1;11)$:

для $q_f = q_f(t_н)$: $\max\left(K_i\right) = 4880,359905$;

для $q_c = q_c(t_н)$: $\max\left(K_i\right) = 30,411511$.

Таблиця 6 – **Порівняльні значення для** $q_f(t_н)$

$t_н$	$q^e{}_f(t_н)$	$q^p{}_f(t_н)$	$\theta = \left\|q^e_f(t_н) - q^p_f(t_н)\right\|$	$t_н$	$q^e{}_f(t_н)$	$q^p{}_f(t_н)$	$\theta = \left\|q^e_f(t_н) - q^p_f(t_н)\right\|$
0	0	0	0	0,249	93	65,743882	27,256118
0,168	81	62,547827	18,45217	0,333	61	67,844585	6,844585
0,188	80	63,809242	16,19076	0,446	83	78,745219	4,254781
0,206	39	64,596778	25,596778	0,849	762	538,115125	223,884875
0,238	92	65,508850	26,49115	0,957	777	478,499059	298,500941
0,241	45	65,575300	20,5753	1	306	306	0

Таблиця 7 – **Порівняльні значення для** $q_c(t_н)$

$t_н$	$q^e{}_c(t_н)$	$q^p{}_c(t_н)$	$\theta = \left\|q^e_c(t_н) - q^p_c(t_н)\right\|$	$t_н$	$q^e{}_c(t_н)$	$q^p{}_c(t_н)$	$\theta = \left\|q^e_c(t_н) - q^p_c(t_н)\right\|$
0	0	0	0	0,249	2	1,335418	0,664582
0,168	1	1,337389	0,337389	0,333	1	1,221982	0,221982
0,188	3	1,360285	1,639715	0,446	1	1,125939	0,125939
0,206	0	1,364959	1,364959	0,849	0	0,731249	0,731249
0,238	2	1,346917	0,653083	0,957	0	1,860081	1,860081
0,241	0	1,343984	1,343984	1	3	3	0

Висновки

Таким чином, в роботі було розроблено математичну модель аналізу кількості успішної та негативної валідацій за час раціонального циклу валідації виявлених вразливостей під час автоматизованого активного аналізу захищеності корпоративної мережі. Слід відзначити, що через неможливість використання диференційних рівнянь було використано поліноми Бернштейна, які успішно апроксимують аналітичні залежності для кількості успішно валідованих вразливостей, невалідованих вразливостей та кількості випадків валідації вразливостей, що призвели до критичних помилок. При цьому виникає певне відхилення через те, що в ході дослідження було взято невелику кількість доданків, однак це є допустимим.

Список літератури

1. Obes J., Richarte G., Sarraute C. Attack planning in the real world. arXiv 2013, arXiv:1306.4044. URL: https://arxiv.org/abs/1306.4044
2. Sarraute C.; Buffet O.; Hoffmann J. Penetration testing = POMDP solving? arXiv 2013, arXiv:1306.4714. URL: https://arxiv.org/abs/1306.4714
3. Shmaryahu D. Partially observable contingent planning for penetration testing / D. Shmaryahu, G. Shani, J. Hoffmann // 2017 1st Int Workshop on Artificial Intelligence in Security. – 2017. – P.33-40. URL: https://cyber.bgu.ac.il/wp-content/uploads/2017/10/IWAISe-17_paper_8-ds.pdf
4. Stefinko Ya.Ya., Piskozub, A.Z. Theory of modern penetration testing expert system. *Information Processing Systems*. 2017. Vol. 2(148). P. 129-133. DOI: https://doi.org/10.30748/soi.2017.148.25.
5. Qiu X., Wang S., Jia Q., Xia C., Lv L. Automatic generation algorithm of penetration graph in penetration testing. *Proc.of the 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. IEEE. 2014. P. 531-537.
6. Steinmetz M. Critical constrained planning and an application to network penetration testing. *26th Int Conf on Automated Planning and Scheduling*. 2016. P. 141-144.
7. Hoffman J. Simulated Penetration Testing: From "Dijkstra" to "Turing Test++". *ICAPS 2015 Proceedings.Published by The AAAI Press*. Palo Alto, CA. 2015.
8. Armitage. URL: https://www.offensive-security.com/metasploit-unleashed/armitage/
9. Browser Market Share. URL: https://netmarketshare.com/
10. Operating System Market Share Ukraine. URL: https://gs.statcounter.com/os-market-share/all/ukraine
11. Малозёмов В. Н. О многочленах Бернштейна. *Семинар «CNSA & NDO». Избранные доклады*. 17.09.2019. 8с.

References

1. Obes, J., Richarte, G. and Sarraute, C. (2013), "Attack planning in the real world", *arXiv*, arXiv:1306.4044, available at: https://arxiv.org/abs/1306.4044
2. Sarraute, C., Buffet, O. and Hoffmann, J. (2013), "Penetration testing = POMDP solving?", *arXiv*, arXiv:1306.4714, available at: https://arxiv.org/abs/1306.4714
3. Shmaryahu, D. Shani, G. and Hoffmann J. (2017), "Partially observable contingent planning for penetration testing", *2017 1st Int Workshop on Artificial Intelligence in Security*, pp. 33-40, available at: https://cyber.bgu.ac.il/wp-content/uploads/2017/10/IWAISe-17_paper_8-ds.pdf
4. Stefinko, Ya.Ya. and Piskozub, A.Z. (2017), "Theory of modern penetration testing expert system", *Information Processing Systems*, Vol. 2(148), pp. 129-133, DOI: https://doi.org/10.30748/soi.2017.148.25.
5. Qiu, X., Wang, S., Jia, Q., Xia, C., and Lv, L. (2014), "Automatic generation algorithm of penetration graph in penetration testing", Pr*oc.of the 2014 Ninth Int. Conf. on P2P*, Parallel, Grid, Cloud and Internet Computing, IEEE, P. 531-537.
6. Steinmetz, M. (2016), "Critical constrained planning and an application to network penetration testing", *26th Int Conf on Automated Planning and Scheduling*, pp. 141-144.

7. Hoffman, J. (2015), “Simulated Penetration Testing: From “Dijkstra” to “Turing Test++”, *ICAPS 2015 Proceedings. Published by The AAAI Press, Palo Alto, CA*.
8. (2020), *Armitage*, available at: https://www.offensive-security.com/metasploit-unleashed/armitage/
9. (2020), *Browser Market Share*, available at: https://netmarketshare.com/
10. (2020), *Operating System Market Share Ukraine*, available at: https://gs.statcounter.com/os-market-share/all/ukraine
11. Malozyomov, V.N. (2019), *On Bernstein Polynomials*, Seminar "CNSA & NDO". Selected papers, 8 p.

Надійшла (received) 14.07.2020
Прийнята до друку (accepted for publication) 09.09.2020

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Киричок Роман Васильович – аспірант, асистент кафедри інформаційної та кібернетичної безпеки, Державний університет телекомунікацій, Київ, Україна;
Roman Kyrychok – postgraduate student, assistant of information and cybersecurity department, State University of Telecommunications, Kyiv, Ukraine;
e-mail: kyrychokr@gmail.com; ORCID ID: http://orcid.org/0000-0002-9919-9691.

Шуклін Герман Вікторович – кандидат технічних наук, завідувач кафедри систем інформаційного та кібернетичного захисту, Державний університет телекомунікацій, Київ, Україна;
Herman Shuklin – Candidate of Technical Sciences, Head of Information and cyber defense systems Department, State University of Telecommunications, Kyiv, Ukraine;
e-mail: mathacadem-kiev@ukr.com; ORCID ID: http://orcid.org/0000-0003-2507-384X.

Барабаш Олег Володимирович – доктор технічних наук, професор, завідувач кафедри вищої математики, Державний університет телекомунікацій, Київ, Україна;
Oleg Barabash – Doctor of Technical Sciences, Professor, Head of the Mathematics Department, State University of Telecommunications, Kyiv, Ukraine;
e-mail: bar64@ukr.net; ORCID ID: http://orcid.org/0000-0003-1715-0761.

Гайдур Галина Іванівна – доктор технічних наук, професор, завідувач кафедри інформаційної та кібернетичної безпекии, Державний університет телекомунікацій, Київ, Україна;
Galyna Gaidur – Doctor of Technical Sciences, Professor, Head of the Department of information and cybersecurity, State University of Telecommunications, Kyiv, Ukraine;
e-mail: gaydurg@gmail.com; ORCID ID: http://orcid.org/0000-0003-0591-3290.

Modeling the vulnerabilities validation mechanism in the active analysis of the security of corporate networks using Bernstein polynomials

Roman Kyrychok, Herman Shuklin, Oleg Barabash, Galyna Gaidur

Abstract. The subject of the article is the models of the process of active analysis of the security of information systems and networks, in particular, one of its key components, namely the vulnerability validation mechanism. **The purpose of the article** is to develop a mathematical model for analysing the number of successful and negative validations over a rational cycle of validation of identified vulnerabilities during an automated active analysis of the security of the corporate network. **Results:** Based on the observations and studies of the exploitation tools of the identified vulnerabilities, it was decided to describe the dynamic of the validation processes using Bernstein polynomials, which successfully approximate the analytical dependencies for the quantitative characteristics of the vulnerability validation process. Also based on a comparison of the empirical and calculated values of these characteristics, it was established that deviations are permissible. **Conclusions:** The developed mathematical model provides with analytical dependencies for the number of successfully validated, invalidated vulnerabilities and the number of vulnerability validation cases that led to critical errors over the rational cycle of validation of identified vulnerabilities.

Keywords: active analysis of the security; vulnerability validation; corporate network; Bernstein polynomial.

Моделирование механизма валидации уязвимостей при активном анализе защищенности корпоративных сетей с помощью полиномов Бернштейна

Р. В. Киричок, Г. В. Шуклин, О. В. Барабаш, Г. И. Гайдур

Аннотация. Предметом изучения статьи есть модели процесса активного анализа защищенности информационных систем и сетей, в частности одного из его ключевых компонентов, а именно механизма валидации уязвимостей. **Целью** исследования является разработка математической модели анализа количества успешной и негативной валидаций за время рационального цикла валидации выявленных уязвимостей во время автоматизированного активного анализа защищенности корпоративной сети. **Результаты:** на основе проведенных в работе наблюдений и исследований функционирования средств эксплуатации выявленных уязвимостей было принято решение об описания динамики процессов валидации именно с помощью полиномов Бернштейна, которые успешно аппроксимируют аналитические зависимости для количественных характеристик процесса валидации уязвимостей. При этом, на основе сравнения эмпирических и расчетных значений данных характеристик установлено, что отклонения допустимы. **Выводы:** разработана математическая модель обеспечивает получение аналитических зависимостей для количества успешно валидированных, невалидованих уязвимостей и количества случаев валидации уязвимостей, которые привели к критическим ошибкам за время рационального цикла валидации выявленных уязвимостей.

Ключевые слова: активный анализ защищенности; валидация уязвимостей; корпоративная сеть; полиномы Бернштейна.