Key words: information system, protection system, adaptation, prioritization, threats, attacks, vulnerabilities, risks, risk-based approach, reflexive model, protection paradigm.

Архипов Олександр Євгенійович, д.т.н., професор, професор кафедри інформаційної безпеки НТУУ «КПІ імені Ігоря Сікорського».
E-mail: sonet0515@gmail.com.
Orcid ID: 0000-0001-6832-2223.

Архипов Александр Евгеньевич, д.т.н., профессор, профессор кафедры информационной безопасности НТУУ «КПИ имени Игоря Сикорского».

Arkhypov Olexander Evgeniyovich, Dr.Sci.Tech., professor at the Department of Information Defense, NTUU «Igor Sikorsky Kyiv Polytechnic Institute».

DOI: 10.18372/2410-7840.23.15431
УДК 004.056

УДОСКОНАЛЕНИЙ МЕТОД АВТОМАТИЧНОГО АКТИВНОГО АНАЛІЗУ ЗАХИЩЕНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ

Роман Киричок, Ольга Зінченко, Ірина Срібна, Віталій Марченко, Олег Кітура

У статті запропоновано удосконалений метод автоматичного активного аналізу захищеності корпоративної мережі. В основу даного методу покладено синтез математичної моделі аналізу кількісних характеристик процесу валідації вразливостей, методики аналізу якості роботи механізму валідації виявлених вразливостей корпоративної мережі та методу побудови нечіткої бази знань для прийняття рішень при валідації вразливостей програмних та апаратних платформ. Зокрема математична модель аналізу ґрунтується на поліномах Бернштейна та дозволяє описати динаміку процесу валідації вразливостей. Методика аналізу якості роботи базується на інтегральних рівняннях, що враховують кількісні характеристики досліджуваного механізму валідації вразливостей в певний момент часу, що дозволяє будувати закони розподілу показників якості процесу валідації вразливостей та кількісно оцінювати якість роботи механізму валідації виявлених вразливостей. Метод побудови нечіткої бази знань базується на використанні нечіткої логіки, що в свою чергу, дає можливість забезпечити отримання достовірної інформації про якість механізму валідації вразливостей непрямим шляхом та дозволяє формувати вирішальні правила прийняття рішень щодо реалізації тієї чи іншої атакуючої дії під час проведення активного аналізу захищеності корпоративної мережі. Це дозволяє, на відміну від існуючих підходів щодо автоматизації активного аналізу захищеності, абстрагуватися від умов динамічної зміни середовища, тобто постійного розвитку інформаційних технологій, що призводить до зростання кількості вразливостей та відповідних векторів атак, а також зростання готових до використання експлойтів вразливостей та їх доступності, і враховувати лише параметри якості самого процесу валідації вразливостей.

Ключові слова: *активний аналіз захищеності, корпоративна мережа, цільова система, валідація вразливостей, експлойт.*

ВСТУП

На сьогодні, одним із актуальних напрямів забезпечення кібербезпеки інформаційних систем та мереж є впровадження превентивних механізмів, серед який, найперспективнішими залишаються методи активного аналізу захищеності, що дозволяють не лише виявляти вразливості, але й валідувати їх, тобто підтверджувати можливість реалізації конкретної вразливості. При цьому, основними недоліками активного аналізу захищеності залишається обробка великого об'єму інформації, яка здебільшого здійснюється вручну експертами або звичайними адміністраторами, а відповідно і якість аналізу залежить від їхньої кваліфікації. Ще одним із недоліків, що є особливо критичним при аналізі захищеності великих мереж, зокрема корпоративних, це масовість перевірок знайдених вразливостей, що відповідно також призводить до збільшення загального часу проведення такого аналізу. Таким чином, враховуючи вищезазначені недоліки, набирає вагомості питання автоматизації процесу активного аналізу захищеності корпоративних мереж, зокрема процедури валідації виявлених вразливостей.

Аналіз останніх публікацій та досліджень свідчить про те, що питанням автоматизації процесу активного аналізу захищеності корпоратив-

них мереж активно займаються, як українські, так і закордонні вчені.

І хоча для вирішення даного питання було запропоновано низку підходи з використанням різних математичних апаратів, зокрема, графів атак [7, 14], марківських процесів прийняття рішень [5], частково спостережуваних марківських процесів прийняття рішень [10-12], мереж Петрі [15] та інші [13], їхня ефективність залишається низькою, через:

- складність підтримки актуальної моделі результатів виконання будь-яких дій в умовах динамічної зміни середовища (проблема масштабованості);
- підвищений ризик повного виведення з ладу цільової системи під час валідації виявлених вразливостей інформаційних систем;
- невирішене питання отримання якісних даних для навчання у разі використання класичних методів машинного навчання.

У зв'язку з цим, подальше удосконалення методу автоматичного активного аналізу захищеності корпоративних мереж є досить актуальним науковим завданням.

Метою статті є удосконалення методу автоматичного активного аналізу захищеності корпоративних мереж на основі оцінювання якості механізму валідації вразливостей функціонуючих інформаційних систем та інтелектуалізації процесу валідації виявлених вразливостей.

ПОСТАНОВКА ЗАДАЧІ

Оскільки існуючі методи автоматизації процесу активного аналізу захищеності корпоративних мереж мають суттєві недоліки, а необхідність оперативного (в режимі реального часу), якісного виявлення та підтвердження вразливостей корпоративних мереж є досить гострою, основною задачею даного дослідження є синтез запропонованих: математичної моделі аналізу кількісних характеристик процесу валідації вразливостей [2], методики аналізу якості роботи механізму валідації виявлених вразливостей корпоративної мережі [1] та методу побудови нечіткої бази знань для прийняття рішень при валідації вразливостей програмних та апаратних платформ [6].

ОСНОВНА ЧАСТИНА

Загалом, методу автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей можна поділити на 4 основних етапи: (I) підготовчий етап, (II) етап ініціалізації, (III) етап адаптивної валідації ймовірних вразливостей, (IV) етап обробки та відображення результатів (визначення фактичного рівня захищеності).

Узагальнене алгоритмічне представлення розробленого методу автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей представлено на рис. 1. Слід відзначити, що запропонований метод включає два режими роботи, перший це навчання, в ході якого здійснюється побудова та адаптація бази знань, а також вирішальних правил, тобто здійснюється «навчання» автоматичної системи активного аналізу захищеності корпоративних мереж, та другий режим – безпосередньо сам активний аналіз захищеності корпоративної мережі.

Окрім цього, на основі проведеного аналізу останніх публікацій та досліджень щодо проведення активного аналізу захищеності корпоративних мереж та методів і засобів його автоматизації відповідно, було сформовано ряд моделей, що дозволяють в якості вхідних даних використовувати інформацію про цільову корпоративну мережу, зокрема інформацію про всі її компоненти, знайдені вразливості та доступні для їх реалізації експлойти.

Структура даних моделей описується за допомогою теоретико-множинного підходу. Далі більш докладно розглянута послідовність кроків запропонованого методу:

Крок 1. Збір інформації щодо цільової корпоративної мережі та формування моделі CN згідно (1). В якості джерела всієї необхідної інформації, зокрема інформації щодо конфігурації окремих хостів цільової корпоративної мережі, може бути використано будь-який сучасний сканер безпеки.

Виходячи з аналізу роботи різноманітних сканерів безпеки, можна стверджувати, що буде

отримана наступна інформацій щодо цільового хоста корпоративної мережі в якій проводиться активний аналіз захищеності:

$$CN = \langle H, T_H, I_H \rangle, \quad (1)$$

де $H = \{h_1, ..., h_j\}$ – кінцева множина (к.м.) цільових хостів (вузлів) корпоративної мережі; T_H – тип j-го цільового хоста; I_H – ключова інформація щодо цільового j-го хоста. Тип хоста представляється як: [8]

$$T_H = \{CS, NH, M\}, \quad (2)$$

де CS – комп'ютерна система; NH – мережеве обладнання; M – мобільна платформа.

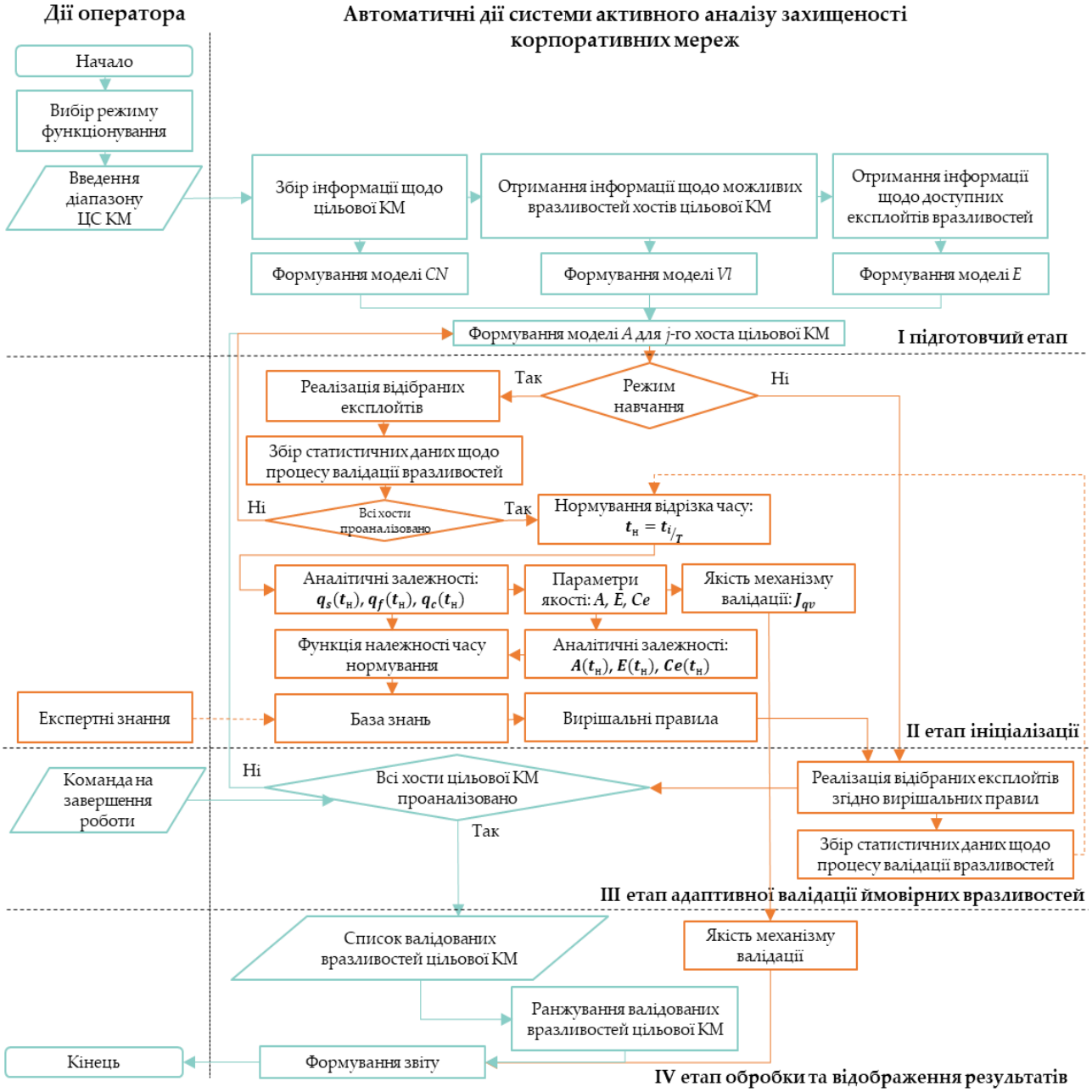

Рис. 1. Алгоритм методу автоматичного активного аналізу захищеності корпоративних мереж на основі інтелектуальної валідації вразливостей

Інформація щодо цільового хоста:

$$I_H = \{Pl, V_{Pl}, S, V_S, P\}, \quad (3)$$

де $Pl = \{pl_1, ..., pl_j\}$ – к.м. платформ (Windows, Linux, Android та інші); $V_{Pl} = \{v_{pl_1}, ..., v_{pl_j}\}$ – к.м.

ймовірних версій платформи; $S=\{s_1,...,s_j\}$ – к.м. сервісів; $V_S=\{v_{s_1},...,v_{s_j}\}$ – к.м. ймовірних назв та версій відповідних сервісів; $P=\{p_1,...,p_j\}$ – к.м. портів на яких запущені та працюють сервіси.

Слід зазначити, що даний опис побудований згідно з стандартом Common Platform Enumeration (CPE) [9], що дозволяє в подальшому, при висуванні припущення щодо наявності вразливостей в цільовій системі, зв'язати конфігурацію хоста з даними із бази вразливостей та підібрати відповідні експлойти.

Крок 2. Отримання інформації щодо можливих вразливостей хостів цільової корпоративної мережі та формування моделі Vl згідно (4).

Основним джерелом інформації щодо вразливостей слугують інтегровані бази вразливостей до засобів активного аналізу захищеності, а також відкриті (в мережі Інтернет) бази вразливостей:

$$Vl=\langle ID_{Vl},R_{Vl},C_{Vl}\rangle, \quad (4)$$

де $ID_{Vl}=\{id_{vl_1},...,id_{vl_n}\}$ – к.м. ідентифікаторів вразливостей представлених в структурованій базі вразливостей MITRE CVE List [4]; $R_{Vl}=\{r_{vl_1},...,r_{vl_n}\}$ – к.м. оцінок критичності вразливостей згідно з CVSS; $C_{Vl}=\{c_{vl_1},...,c_{vl_n}\}$ – к.м. відомих вразливих конфігурацій (ідентифікаторів оформлених за допомогою Common Platform Enumeration).

Крок 3. Отримання інформації щодо доступних експлойтів та формування моделі E згідно (5).

Відповідно джерелом необхідної інформації є відкриті та закриті (зокрема, платні) бази експлойтів, готові exploitkit-набори або інтегровані бази готових до використання експлойтів вразливостей безпосередньо самих засобів експлуатації

$$E=\langle N_E,D_E,R_E,Rf_E\rangle, \quad (5)$$

де $N_E=\{n_{E_1},...,n_{E_g}\}$ – к.м. коротких назв доступних експлойтів (фактично ідентифікатори представлені тим чи іншим засобом експлуатації); $D_E=\{d_{E_1},...,d_{E_g}\}$ – к.м. коротких описів експлойтів (в яких вказується назва та версія вразливого сервісу); $R_E=\{excellent,...,manual\}$ – к.м. рангів якості експлойтів, детальний опис яких представлено в [3]; $Rf_E=\{rf_{E_1},...,rf_{E_g}\}$ – к.м. посилань на ідентифікатори вразливостей, які реалізуються за допомогою експлойта.

Крок 4. Відбір експлойтів вразливостей для *j*-го хоста цільової мережі згідно з моделлю кібератаки A (з використанням вразливостей), яка формується на основі відповідності основним визначеним характеристикам та вразливостям цільової системи:

$$A=\{a_1,...,a_k\}, \quad (6)$$

де $a_k=F\begin{pmatrix}((Vl.C_{Vl},I_H.S,I_H.V_S)\&(E.Rf_E,Vl.ID_{Vl}))\\|(E.D_E,I_H.S,I_H.V_S)\end{pmatrix}$.

Крок 5 (в режимі навчання). Здійснюється почергова реалізація відібраних експлойтів та збір статистичних даних щодо базових характеристик процесу валідації вразливостей цільового хоста. На основі зібраних даних, здійснюється оцінка якості механізму валідації вразливостей за наступними підкроками:

5.1. Нормування відрізка часу проведення валідації вразливостей хостів цільової корпоративної мережі згідно (7):

$$t_н=\frac{t_i}{T}. \quad (7)$$

5.2. Отримання аналітичних залежностей для базових характеристик (q_s,q_f,q_c) процесу валідації вразливостей (8):

$$q_s(t_н)=\sum_{i=0}^{n}q_s(t_н^{(i)})b_{k,n}(t_н),$$
$$q_f(t_н)=\sum_{i=0}^{n}q_f(t_н^{(i)})b_{k,n}(t_н),$$
$$q_c(t_н)=\sum_{i=0}^{n}q_c(t_н^{(i)})b_{k,n}(t_н). \quad (8)$$

5.3. Розрахунок показників якості механізму валідації вразливостей (9): A - акуратності, E – похибки та Ce – критичної помилки.

$$A=\frac{\int_0^1 q_s(\theta)d\theta}{\int_0^1(q_s(\theta)+q_f(\theta)+q_c(\theta))d\theta},$$

$$E = \frac{\int_0^1 q_f(\theta)d\theta}{\int_0^1 (q_s(\theta)+q_f(\theta)+q_c(\theta))d\theta},$$

$$Ce = \frac{\int_0^1 q_c(\theta)d\theta}{\int_0^1 (q_s(\theta)+q_f(\theta)+q_c(\theta))d\theta}. \quad (9)$$

5.4. Оцінка якості механізму валідації виявлених вразливостей програмних та апаратних платформ цільової корпоративної мережі згідно з єдиним інтегральним показником якості (10).

$$J_{qv} = \frac{A}{E} - Ce. \quad (10)$$

5.5. Побудова законів розподілу для показників якості механізму валідації вразливостей $A(t_н)$, $E(t_н)$, $Ce(t_н)$ згідно (11):

$$A(t_н) = \frac{\int_0^{t_н} q_s(\theta)d\theta}{\int_0^{t_н} (q_s(\theta)+q_f(\theta)+q_c(\theta))d\theta},$$

$$E(t_н) = \frac{\int_0^{t_н} q_f(\theta)d\theta}{\int_0^{t_н} (q_s(\theta)+q_f(\theta)+q_c(\theta))d\theta},$$

$$Ce(t_н) = \frac{\int_0^{t_н} q_c(\theta)d\theta}{\int_0^{t_н} (q_s(\theta)+q_f(\theta)+q_c(\theta))d\theta}. \quad (11)$$

5.6. Побудова функції належності часу нормування згідно отриманих статистичних даних;

5.7. Побудова бази знань та подальше формування вирішальних правил прийняття рішень щодо реалізації атакуючої дії з врахуванням рангу якості експлойта, який надається засобом експлуатації вразливостей. Зокрема, попередньо визначивши необхідну кількість правил логічного висновку вигляду $R(i)$: *ЯКЩО* $(A_i \in T \,\&\, E_i \in T \,\&\, Ce_i \in T)$ $TO(Q_{mv_i} \in T), i = \overline{1,k}$ згідно (12).

$$N_{\max} = I_1 \cdot I_2 \cdot \ldots \cdot I_n. \quad (12)$$

Крок 5 (в режимі активного аналізу). Реалізація відібраних експлойтів у відповідності до вирішальних правил прийняття рішень та збір статистичних даних щодо процесу валідації вразливостей, на основі чого, згідно з *кроками 5.1-5.4* здійснюється оцінка якості механізму валідації вразливостей;

Крок 6 (в режимі активного аналізу). Ранжування валідованих вразливостей цільової корпоративної мережі та формування звіту проведеного активного аналізу захищеності.

Проаналізувавши всі хости цільової корпоративної мережі, формується загальний список валідованих, тобто підтверджених вразливостей, водночас здійснюється їх ранжування у відповідності до рівня їхньої критичності, яка визначена базовою оцінкою CVSS та рівня розповсюдженості даної вразливості L_{v_i} в корпоративній мережі згідно виразу (13), в іншому випадку, відбувається повернення до кроку 5 (в режимі активного аналізу).

В результаті, формується звіт проведеного активного аналізу захищеності, що містить відранжований перелік підтверджених вразливостей цільової корпоративної мережі в порядку убування, від вразливостей з найвищими рівнями критичності та розповсюдженості до вразливості з найнижчими рівнями, а також рівень якості механізму валідації виявлених вразливостей

$$L_{v_i} = \frac{h_v}{h_T} \cdot 100, \quad (13)$$

де h_v – кількість вразливих хостів до валідованої вразливості v.

h_T – загальна кількість проаналізованих хостів цільової корпоративної мережі, $h_T > 0$.

На основі звіту, оператор приймає рішення щодо першочергового усунення тієї чи іншої валідованої вразливості з метою забезпечення визначеного рівня безпеки. Окрім цього, оператор також приймає рішення щодо необхідності, у разі занадто низького рівня якості роботи механізму валідації вразливостей, «перенавчання» автоматизованої системи активного аналізу захищеності в ході якого проводиться адаптація побудованої бази знань та сформованих вирішалиних правил прийняття рішень.

ВИСНОВКИ

Таким чином, в роботі було удосконалено метод автоматичного активного аналізу захищеності корпоративної мережі. Особливість запропонованого методу полягає в можливості абстрагування від умов динамічної зміни середовища, тобто постійного розвитку інформаційних технологій, що призводить до зростання кількості вразливостей та відповідних векторів атак, а також зростання готових до використання експлойтів вразливостей та їх доступності, і враховуючи лише параметри якості самого процесу валідації вразливостей. При цьому, задача автоматизації процесу валідації вразливостей була вирішена шляхом інтелектуалізації процесу валідації вразливостей програмних та апаратних платформ на основі фаззі-технології.

ЛІТЕРАТУРА

[1] Киричок Р.В. Методика аналізу якості роботи механізму валідації вразливостей корпоративних мереж / Р.В. Киричок, Г.В. Шуклін // *Телекомунікаційні та інформаційні технології*. – 2020. – №2(67). С. 29-40.

[2] Киричок Р.В. Моделювання механізму валідації вразливостей при активному аналізі захищеності корпоративних мереж за допомогою поліномів Бернштейна // Р.В. Киричок, Г.В. Шуклін, О.В. Барабаш, Г.І. Гайдур / *Сучасні інформаційні системи*. – 2020. – Том 4, №3. С. 118-123.

[3] Chapple M. *CompTIA PenTest+ Study Guide: Exam PT0-001* / M. Chapple, D. Seidl // CompTIA. – 2018. – 544 p.

[4] *Common Vulnerabilities and Exposures* [Електронний ресурс] – Режим доступу: http://cve. mitre.org/.

[5] Durkota K. Computing optimal policies for attack graphs with action failures and costs / K. Durkota, V. Lisy // In *7th European Starting AI Researchers` Symposium «STAIRS'14»* Vol. 264, January 2014. pp. 101-110.

[6] Kyrychok R. The method of building a knowledge base for dicision-making when validating corporate networks vulnerabilities / R. Kyrychok, G. Shuklin // *Scientific Discussion*. – 2020. – Vol. 1, №47. – pp. 7-11.

[7] Luan J. Automated Vulnerability Modeling and Verification for Penetration Testing Using Petri Nets / J. Luan, J. Wang, M. Xue // Cloud Computing and Security. ICCCS 2016. *Lecture Notes in Computer Science*. July 2016. Vol. 10040. – 502 p.

[8] Monahan G.E. State of the art – a survey of partially observable Markov decision processes: theory, models, and algorithms / G. E. Monahan // *Manage. Sci.* – 1982. – vol.28, №1. – pp. 1–16.

[9] *National Vulnerability Database* [Електронний ресурс] – Режим доступу: https://nvd.nist.gov/.

[10] *C. Penetration testing POMDP solving?* / C. Sarraute, O. Buffet, J. Hoffmann // arXiv 2013, arXiv:1306.4714. [Електронний ресурс]. – Режим доступу: https://arxiv.org/abs/1306.4714.

[11] Sarraute C. POMDPs make better hackers: Accounting for uncertainty in penetration testing / C. Sarraute, O. Buffet, J. Hoffmann// In Proceedings of the *26th AAAI Conference on Artificial Intelligence «AAAI'12»*. July 2012. – Toronto, ON, Canada: AAAI Press, 2012. -pp. 1816-1824.

[12] 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. – pp.33-40.

[13] Sutton R.S. *Reinforcement Learning: An Introduction second edition.* / R.S. Sutton, A.G. Barto // The MIT Press, Cambridge, MA, 2018. - 445 p.

[14] Qiu X. Automatic generation algorithm of penetration graph in penetration testing / X. Qiu, S. Wang, Q. Jia, C. Xia and L. Lv // In Proceedings of the 2014 *Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, IEEE. November 8-10, 2014. – Guangdong, China, 2014. – pp. 531-537.

[15] Wu D. A security threats identification and analysis method based on attack graph/D. Wu, Y.-F. Lian, K. Chen, Y.-L. Liu//*Jisuanji Xuebao (Chinese Journal of Computers)*, 2012. – Vol. 35, №. 9. – pp. 1938–1950.

УСОВЕРШЕНСТВОВАННЫЙ МЕТОД АВТОМАТИЧЕСКОГО АКТИВНОГО АНАЛИЗА ЗАЩИЩЕННОСТИ КОРПОРАТИВНОЙ СЕТИ

В статье предложен усовершенствованный метод автоматического активного анализа защищенности корпоративной сети. В основу данного метода положен синтез математической модели анализа количественных характеристик процесса валидации уязвимостей, методики анализа качества работы механизма валидации выявленных уязвимостей корпоративной сети и метода построения нечеткой базы знаний для принятия решений при валидации уязвимостей программных и аппаратных платформ. В частности, математическая модель анализа основывается на полиномах Бернштейна и позволяет описать динамику процесса валидации уязвимостей. Методика анализа качества работы базируется на интегральных уравнениях, учитывающие количественные характеристики исследуемого механизма валидации уязвимостей в определенный момент времени, что позволяет строить законы распределения показателей качества процесса валидации уязвимостей и количественно оценивать качество работы механизма валидации выявленных уязвимостей. Метод построения нечеткой базы знаний базируется на использовании нечеткой логики, что в свою очередь, дает возможность обес-

печить получение достоверной информации о качестве механизма валидации уязвимостей косвенным путем и позволяет формировать решающие правила принятия решений по реализации того или иного атакующего действия во время проведения активного анализа защищенности корпоративной сети. Это позволяет, в отличие от существующих подходов к автоматизации активного анализа защищенности, абстрагироваться от условий динамического изменения среды, то есть постоянного развития информационных технологий. Это приводит к росту количества уязвимостей и соответствующих векторов атак, а также росту готовых к использованию эксплойтов уязвимостей и их доступности, учитывая только параметры качества самого процесса валидации уязвимостей.

Ключевые слова: активный анализ защищенности, корпоративная сеть, целевая система, валидация уязвимостей, эксплойт.

IMPROVED METHOD OF AUTOMATIC ACTIVE ANALYSIS OF CORPORATE NETWORK SECURITY

The article proposes an improved method for automatic active analysis of corporate network security. This method is based on the synthesis of a mathematical model for analyzing the quantitative characteristics of the vulnerability validation process, a methodology for analyzing the quality of the validation mechanism for identified vulnerabilities in a corporate network, and a method for constructing a fuzzy knowledge base for making decisions when validating vulnerabilities of software and hardware platforms. In particular, the mathematical analysis model, that is based on Bernstein polynomials, allows describing the dynamics of vulnerability validation process. A methodology for analysing the quality of work is based on integral equations that take into account the quantitative characteristics of the investigated vulnerability validation mechanism at a certain point in time, which makes it possible to build laws for the distribution of quality indicators of the vulnerability validation process and quantitatively assess the quality of the validation mechanism for the identified vulnerabilities. The method of building a fuzzy knowledge base is based on the use of fuzzy logic which makes it possible to obtain reliable information about the quality of the vulnerability validation mechanism in an indirect way and allows the formation of final decision-making rules for the implementation of one or another attacking action during the active security analysis of corporate network. This allows, in contrast to existing approaches to automating active security analysis, to abstract from the conditions of dynamic changes in the environment, that is, the constant development of information technologies. This leads to an increase in the number of vulnerabilities and corresponding attack vectors, as well as to an increase in ready-to-use exploit vulnerabilities and their availability, taking into account only the quality parameters of the vulnerability validation process itself.

Keywords: active security analysis, corporate network, target system, vulnerability validation, exploit.

Киричок Роман Васильович, старший викладач кафедри Інформаційної та кібернетичної безпеки Державного університету телекомунікацій.
E-mail: kyrychokr@gmail.com.
Orcid ID: 0000-0002-9919-9691.
Киричек Роман Васильевич, старший преподаватель кафедры Информационной и кибернетической безопасности Государственного университета телекоммуникаций.
Kyrychok Roman, Senior lecturer at the Department of Information and Cyber Security, State University of Telecommunications.

Зінченко Ольга Валеріївна, к.т.н., доцент, завідувач кафедри Штучного інтелекту Державного університету телекомунікацій.
E-mail: zinchenkoov@gmail.com.
Orcid ID: 0000-0002-3973-7814.
Зинченко Ольга Валерьевна, к.т.н., доцент, заведующая кафедрой Искусственного интеллекта Государственного университета телекоммуникаций.
Zinchenko Olha, Cand. Sci.Tech., Associate Professor, Head of the Department of Artificial Intelligence, State University of Telecommunications.

Срібна Ірина Миколаївна, к.т.н., доцент, доцент кафедри Інформаційних систем та технологій Державного університету телекомунікацій.
E-mail: isribnaya@gmail.com.
Orcid ID: 0000-0001-9242-2021.
Срибная Ирина Николаевна, к.т.н., доцент, доцент кафедры Информационных систем и технологий Государственного университета телекоммуникаций.
Sribna Iryna, Cand. Sci.Tech., Associate Professor, Associate Professor at the Department of Information Systems and Technologies, State University of Telecommunications.

Марченко Віталій Вікторович, аспірант Державного університету телекомунікацій.
E-mail: vetaldominus@gmail.com.
Orcid ID: 0000-0003-4271-3132.
Марченко Виталий Викторович, аспирант Государственного университета телекоммуникаций.
Marchenko Vitalii, post-graduate student, State University of Telecommunications.

Кітура Олег Володимирович - аспірант, Державний університет телекомунікацій.
E-mail: savitan@ukr.net.
Orcid ID: 0000-0001-6950-4803.
Китура Олег Владимирович, аспирант Государственного университета телекоммуникаций.
Kitura Oleh, post-graduate student, State University of Telecommunications.