УДК 004.056.5 DOI: 10.46972/2076-1546.2019.17.16

В. В. Охрімчук

МЕТОД ПОБУДОВИ ШАБЛОНІВ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ КІБЕРАТАК

На сьогодні у світі спостерігається суттєве збільшення кількості кібератак. При цьому пропорційно зростає їх технологічна складність. У найближчому майбутньому не виключається поява нових потенційно небезпечних кібератак, що, у свою чергу, може призвести до погіршення їх виявлення й нейтралізації та, як наслідок, негативно вплинути на рівень захищеності інформаційних та інформаційно-телекомунікаційних систем критичної інформаційної інфраструктури. З урахуванням зазначеного у статті вирішується актуальне завдання розроблення достовірного методу побудови шаблонів потенційно небезпечних кібератак, упровадження якого забезпечить усунення базового недоліку створення сигнатур шаблонів атак, а саме "ефекту запізнення" з вироблення потрібної сигнатури. В основу запропонованого методу покладено визначення ключових характеристик і параметрів потенційно небезпечної кібератаки, яке здійснюється на підставі аналізу стандартного функціонального профілю захищеності, реалізованого в комп'ютерній системі та мережі, а також джерел первинних даних, які використовуються для побудови шаблонів потенційно небезпечних кібератак. Результатом практичного застосування зазначеного методу є побудова двох шаблонів потенційно небезпечної кібератаки на комп'ютерну систему та мережу. Перший – диференційно-ігровий шаблон потенційно небезпечної кібератаки, що описує фізику процесів, які відбуваються в комп'ютерній системі та мережі під час проведення потенційно небезпечної кібератаки. Другий – фізичний шаблон, що містить у собі повний набір характеристик та параметрів, характерних цій атаці.

Ключові слова: *метод; вразливість; кібератака; кіберзагроза; комп'ютерна система та мережа; система інформаційної безпеки; сигнатура; стандартний функціональний профіль захищеності; шаблон потенційно небезпечної кібератаки.*

Постановка проблеми в загальному вигляді. Широке застосування комп'ютерних систем та мереж (КСМ) у різних сферах, наприклад, економічній, військовій, енергетичній, транспортній тощо, суттєво впливає на ефективність діяльності не тільки окремо взятої людини, але й суспільства та держави в цілому. Проте окрім усіх позитивних ефектів від впровадження КСМ у діяльність сучасного суспільства суттєво й не в кращий бік змінюється ситуація щодо їх безпеки [1, 2]. Так, сьогодні найбільшу небезпеку для них становлять кібератаки (КбА). Актуальність даної проблеми підтверджується статистичними даними за 2018–2019 рр. [1]. До того ж не тільки збільшується їх кількість, а й зростає технологічна складність таких атак. Це, у свою чергу, призводить до погіршення їх виявлення та нейтралізації, що негативно впливає на рівень захищеності КСМ. Відомі на даний час технології, покладені в основу функціонування систем інформаційної безпеки (СІБ) (антивірусних СІБ, систем виявлення КбА), ґрунтуються на використанні сигнатурного методу виявлення КбА. Це, відповідно, призводить до появи так званого "ефекту запізнення", який виникає через часові затримки,

© В. В. Охрімчук, 2019

зумовлені технологічною процедурою розроблення потрібного шаблону (сигнатури) КбА тільки після її виявлення та нейтралізації, що суттєво знижує захищеність КСМ від нових потенційно небезпечних атак, особливо тих, які мають високу технологічну складність.

Отже, завдання виявлення та нейтралізації потенційно небезпечних КбА на КСМ набуває особливої актуальності та може бути вирішене шляхом розроблення нових дієвих та модифікацією відомих методів побудови шаблонів КбА.

Аналіз останніх досліджень і публікацій [1–8] показав, що, незважаючи на значну кількість КСМ, проблема їх безпеки й надалі залишається актуальною, з нею також пов'язані питання технологічного [9], організаційного [10], дефініційного [11] характеру тощо.

У технологічному сенсі сьогодні відбувається комплексування відомих підходів до побудови сигнатур шаблонів атак. Кожен із провідних вендорів антивірусного програмного забезпечення, зокрема Kaspersky Lab, Panda Security, Intel Security-McAfee, ESET, Dr.Web Dr.Web тощо, тримає в комерційній таємниці способи побудови шаблонів атак. Інші відомі підходи, висвітлені в [12, 22], в кожному окремому випадку потребують адаптації.

Організаційна складова проблеми безпеки КСМ обумовлена суперечностями між усталеними у світовій практиці підходами до організації процесу забезпечення захищеності та їх повільною ратифікацією не тільки в межах України, а й усіх країн пострадянського простору.

Дефініційна проблема безпеки є відлунням організаційної. Навіть провідні вчені в галузі безпеки КСМ на сьогодні не мають єдиного бачення на вирішення питання забезпечення технічного захисту інформації на об'єктах інформаційної діяльності, безпеки інформаційних і комунікаційних систем, інформаційної та кібернетичної безпеки як окремої складової безпеки КСМ, так і безпеки системи в цілому.

Як показав критичний аналіз відомих публікацій за темою дослідження, означена вище проблема, незважаючи на її багатогранність, і досі залишається актуальною та потребує свого розв'язання.

Формулювання завдання дослідження. Метою статті є створення достовірного методу розроблення шаблону потенційно небезпечних КбА, що забезпечить відкриття нового дієвого механізму підвищення захищеності КСМ різного цільового призначення.

Виклад основного матеріалу. *Твердження*. Під потенційно небезпечною КбА будемо розуміти таку, яка призводить до порушення нормального функціонування КСМ та, як наслідок, ускладнює або унеможливлює виконання нею завдань за призначенням. При цьому вважається, що відомості про таку КбА в базах даних сигнатур СІБ відсутні.

Зазвичай будь-яка КбА характеризується наявністю невід'ємних складових, які необхідні для досягнення її мети, а саме [13]:

джерело (суб'єкт) атаки – зловмисник, шкідливе програмне забезпечення, за рахунок якого здійснюється КбА;

наявні в КСМ та її компонентах вразливості та варіанти їх використання;

об'єкт КбА, яким можуть бути ресурси КСМ та її компоненти.

Саме визначивши ці складові, можливо буде з високою ймовірністю стверджувати про проведення КбА на КСМ. Отже, метод розроблення шаблонів потенційно

небезпечних КбА повинен бути направлений на визначення їх ключових характеристик і параметрів та містити певні кроки.

Крок 1. Усебічне дослідження та аналіз КСМ

Для розроблення шаблону потенційно небезпечної КбА на першому етапі необхідно визначити її клас та всю множину ресурсів КСМ і її компонентів, які потенційно можуть бути атаковані. З цією метою слід проаналізувати стандартний функціональний профіль захищеності (СФПЗ), реалізований у КСМ. Це в першу чергу пов'язано з тим, що він реалізований для підтримання функціональних спроможностей КСМ, виведення з ладу яких призведе до неможливості використовувати її за призначенням. У результаті дослідження СФПЗ КСМ отримаємо ймовірний клас потенційно небезпечної КбА та множину ресурсів, які потенційно можуть бути атаковані.

Отже, як відомо з [14], СФПЗ – це перелік мінімально необхідних послуг, який повинен реалізовувати комплекс засобів СІБ КСМ, щоб відповідати визначеним вимогам щодо захищеності інформації, яка обробляється в даній КСМ. Таким чином, СФПЗ A, враховуючи зазначене припущення, можна подати в такому вигляді [15]:

$$A = \{a_1, a_2, ...a_\alpha\}, \tag{1}$$

де a_α – мінімально необхідна послуга безпеки, причому $6 \le |A| \le 24$.

Такий діапазон показників обумовлений кількістю мінімально необхідних послуг безпеки, що формують СФПЗ. Відповідно до [14] їх кількість варіюється від 6 до 24 для одного СФПЗ. Як відомо, послуга a_α може включати декілька рівнів. Чим вищий рівень послуги, тим більш повно вона забезпечує захист від певного класу кіберзагроз. Отже, на основі аналізу СФПЗ та його мінімальних необхідних послуг безпеки можливо визначити клас потенційно небезпечної КбА. Це пов'язано з тим, що виведення з ладу однієї з послуг СФПЗ може призвести до порушення функціонування КСМ, тобто до успішного проведення КбА. Якщо основною функцією КСМ є забезпечення доступності користувачів до її ресурсів, то і СФПЗ буде сформований таким чином, щоб її захистити, а отже, і клас потенційно небезпечної КбА повинен бути направлений на порушення цієї доступності.

Кожна послуга є набором функцій, що реалізуються певними ресурсами КСМ, метою яких є протидія визначеній множині загроз. Отже, як було зазначено вище, враховуючи невід'ємні характерні компоненти КбА, для успішного проведення потенційно небезпечної атаки необхідно порушити нормальне функціонування ресурсів КСМ, які забезпечують ту чи іншу мінімально необхідну послугу безпеки СФПЗ.

Таким чином, враховуючи зазначене припущення, з усієї множини ресурсів КСМ $R = \{r_1, r_2, ..., r_k\}$, де k – кількість її ресурсів, можливо визначити підмножину ресурсів R', які можуть бути потенційно атаковані. Як було вказано в [16], будь-який k-й ресурс КСМ r_k можна описати кортежем як

$$r_k = \langle r_k, A_r, V_r, Ch_r \rangle, \tag{2}$$

де r_k – k-й ресурс КСМ;

A_r – множина мінімально необхідних послуг безпеки СФПЗ A, функціонування яких залежить від даного ресурсу, причому $A_r \subseteq A$ та $0 \le |A_r| \le 24$;

V_r – множина вразливостей даного ресурсу;

Ch_r – множина його параметрів та характеристик.

Отже, множина ресурсів R', які можуть бути потенційно атаковані, формується з ресурсів, у яких виконується така умова:

$$|A_r| \neq 0. \tag{3}$$

Тобто обраний ресурс повинен забезпечувати функціонування хоча б однієї мінімально необхідної послуги a_α СФПЗ A.

З урахуванням наведеного вище множина ресурсів КСМ, які можуть бути потенційно атаковані, набуває такого вигляду:

$$R' = \left\{ \left\langle r_k, A_r, V_r, Ch_r \right\rangle \mid r_k \in R, A_r \subseteq A, |A_r| \neq 0 \right\}. \tag{4}$$

У результаті виконання першого кроку методу розроблення шаблонів потенційно небезпечних КбА отримаємо необхідні вихідні дані, які будуть використані на наступних кроках.

Крок 2. Визначення джерел первинних даних для побудови шаблонів потенційно небезпечних КбА

Сьогодні у світі існує достатньо велика кількість вендорів СІБ, що займаються моніторингом, класифікацією та накопиченням відомостей про кіберзагрози. Кожна така організація надає, як правило, відкритий доступ до своїх власних баз кіберзагроз, які заповнюються різноманітною інформацією на свій розсуд. Це призводить до дисбалансу форматів подання первинних даних. Як наслідок, ускладнюються технології їх використання для створення шаблонів КбА. Крім того, дані від таких джерел не завжди комплексуються, що спричиняє нехтування низкою важливих інформативних характеристик, які описують КбА.

Детальний аналіз найбільш поширених баз первинних даних для побудови шаблонів потенційно небезпечних КбА наведено в [17]. Враховуючи ключові складові КбА [13, 16], усі відомі бази даних про них можна поділити на три великі категорії: ті, що характеризують середовище атаки; які описують об’єкт КбА та характеризують суб’єкт атаки.

Як показує практика, для опису середовища атаки найбільшого поширення набула база шаблонів атак KDD-99 [18], що містить $5 \cdot 10^6$ шаблонів мережевих з’єднань, які описують нормальну та аномальну поведінку трафіка в КСМ.

За бази даних, що характеризують суб’єкт атаки, доцільно використовувати ті, які містять у собі опис вразливостей ресурсів КСМ. Однією з найпоширеніших є база даних загальновідомих вразливостей інформаційної безпеки Common Vulnerabilities and Exposures (CVE) [19]. Вона містить множину відомих вразливостей програмних засобів КСМ та СІБ V_{CVE}.

Для опису суб'єкта атаки доцільно використовувати бази даних, які містять у собі шаблони дій зловмисника. Прикладом є база шаблонів КбА CAPEC (Common Attack Pattern Enumeration and Classification) компанії MITRE [20].

Для обрання з усієї множини відомих баз даних необхідно скористатися двома правилами: мінімальна кількість баз даних, які обираються як джерела первинних даних для розроблення шаблонів потенційно небезпечних КбА, має відповідати кількості її складових; обрані бази даних повинні мати максимальну інформативність про складові КбА.

Отже, у результаті виконання другого кроку отримаємо множину баз даних, які будуть використані як джерела первинних даних для розроблення шаблонів потенційно небезпечних КбА.

Крок 3. Оптимізація вихідних даних, необхідних для побудови шаблонів потенційно небезпечних КбА

Оптимізація вихідних даних здійснюється з метою відбору з усієї множини вхідних даних, необхідних для побудови шаблону потенційно небезпечної КбА, конкретних показників та характеристик, що однозначно будуть її визначати.

Оптимізації підлягає кожне джерело первинних даних, обране в ході виконання другого кроку.

Так, якщо для опису станів мережевого трафіка використовують базу KDD-99, то мережевий трафік є набором s вхідних інформативних параметрів, які підлягають контролю, $s = \overline{1,41}$ [21]. В умовах обмеженого часу на побудову шаблону потенційно небезпечної КбА використання визначеної кількості із s параметрів не є раціональним підходом. Доцільним у такому разі є оптимізувати кількість параметрів із s до s', де $s' \le s$. Дане припущення є справедливим, оскільки в [22] визначено найбільш інформативні параметри для усіх класів КбА та доведено, що кожен із відомих, а відповідно, і невідомих класів КбА може бути описаний своєю множиною з s' параметрів, які його чітко визначають.

Метою оптимізації множини ресурсів КСМ, які можуть бути потенційно атаковані R', є виокремлення тих, на які можуть бути спрямовані протиправні дії зловмисника.

Оскільки кожний ресурс $r_k \in R'$ можна подати у вигляді (2), то множина ресурсів, які потенційно можуть бути атакованими, являтиме собою відношення R'', задане на декартовому добутку множин ресурсів КСМ R', та відомих вразливостей V_{CVE} [23]. У формалізованому вигляді воно може бути представлене булевою матрицею суміжності:

R''	v_1	v_2	v_3	$\cdots$	v_n
r_1	1	0	1	$\cdots$	1
r_2	0	0	0	$\cdots$	1
r_3	0	0	1	$\cdots$	1
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$r_{зв}$	1	1	0	$\cdots$	0

. (5)

Таким чином, множина R'' містить упорядковані пари (5). Першим елементом впорядкованої пари є ресурс r_k множини R', що має вразливість, а другим – відповідна цьому ресурсу вразливість $v_n \in V_{CVE}$, тобто

$$R'' \subseteq R' \times V_{CVE} = \left\{ \left\langle r_k, v_n, Ch_r \right\rangle \mid r_k \in R', v_n \in V_{CVE}, r_k R'' v_n \right\}. \quad (6)$$

Така оптимізація дає змогу розглядати два можливі варіанти проведення потенційно небезпечної КбА: перший – атака зловмисника буде націлена на ресурс r_k, який матиме максимальну кількість вразливостей; другий – зловмисник для здійснення потенційно небезпечної КбА буде використовувати вразливість, притаманну максимально можливій множині ресурсів R''.

Оптимізацію параметрів множини вхідних даних, що описують суб'єкт атаки, здійснюють шляхом обрання параметрів, які характеризують дії зловмисника, потенційно можливі для експлуатації обраної вразливості чи здійснення КбА на визначений ресурс.

Отже, у результаті виконання третього кроку отримаємо усі необхідні дані для побудови шаблону потенційно небезпечної КбА.

Крок 4. Побудова шаблонів потенційно небезпечних КбА

На четвертому кроці безпосередньо створюють два шаблони потенційно небезпечної КбА на КСМ. Перший – диференційно-ігровий, він описує фізику процесів, що відбуваються в КСМ під час проведення потенційно небезпечної КбА. Другий – фізичний шаблон, що містить у собі повний набір характеристик та параметрів, притаманних цій атаці.

Для побудови першого шаблону потенційно небезперечної КбА застосуємо диференційно-ігровий метод, описаний у [12]. Для кожного ресурсу $r_k \in R''$ необхідно визначити множину станів, у яких вони можуть перебувати під час здійснення КбА, та проаналізувати переходи з одного стану в інший. За результатами аналізу необхідно побудувати диференційно-ігровий граф шаблону потенційно небезпечної КбА. Опис отриманого графа здійснюється за допомогою диференційних перетворень [24, 25]. Отже, практичне використання диференційно-ігрового шаблону потенційно небезпечної КбА дозволяє вивчати процеси кіберзахисту та кібернападу в КСМ за різних вхідних даних, не проводячи натурного експерименту через його потенційну небезпеку для об'єкта.

Фізичний шаблон потенційно небезпечної КбА формується на основі показників та параметрів, оптимізованих під час виконання кроків 1–3 цього методу, та моделі шаблону потенційно небезпечної КбА, описаної в [16].

У загальному вигляді запропонований метод побудови шаблонів потенційно небезпечної КбА можна подати у вигляді структурної схеми, зображеної на рис. 1. Виконання кроків 1–4 дає змогу встановити факт проведення потенційно небезпечної КбА. Для її виявлення та нейтралізації розроблений метод слід доповнити ще одним кроком (крок 5) (див. рис. 1), який виходить за межі даного дослідження. Метою даного кроку є класифікація потенційно небезпечної КбА.

На сьогодні відомо багато різних підходів до класифікації КбА [26–29]. Вважається, що найбільш повним та систематизованим варіантом, який застосовують на практиці для вирішення низки прикладних завдань, є узагальнена класифікація КбА, розроблена в [27] та подана у формалізованому вигляді в [30]. Перевагою обраного підходу є застосування ознакового принципу для опису різних класів КбА, який забезпечує опис не тільки відомих на сьогодні класів атак, а й дозволяє розширювати ознаковий простір для опису нових, невідомих і, відповідно, потенційно небезпечних класів.

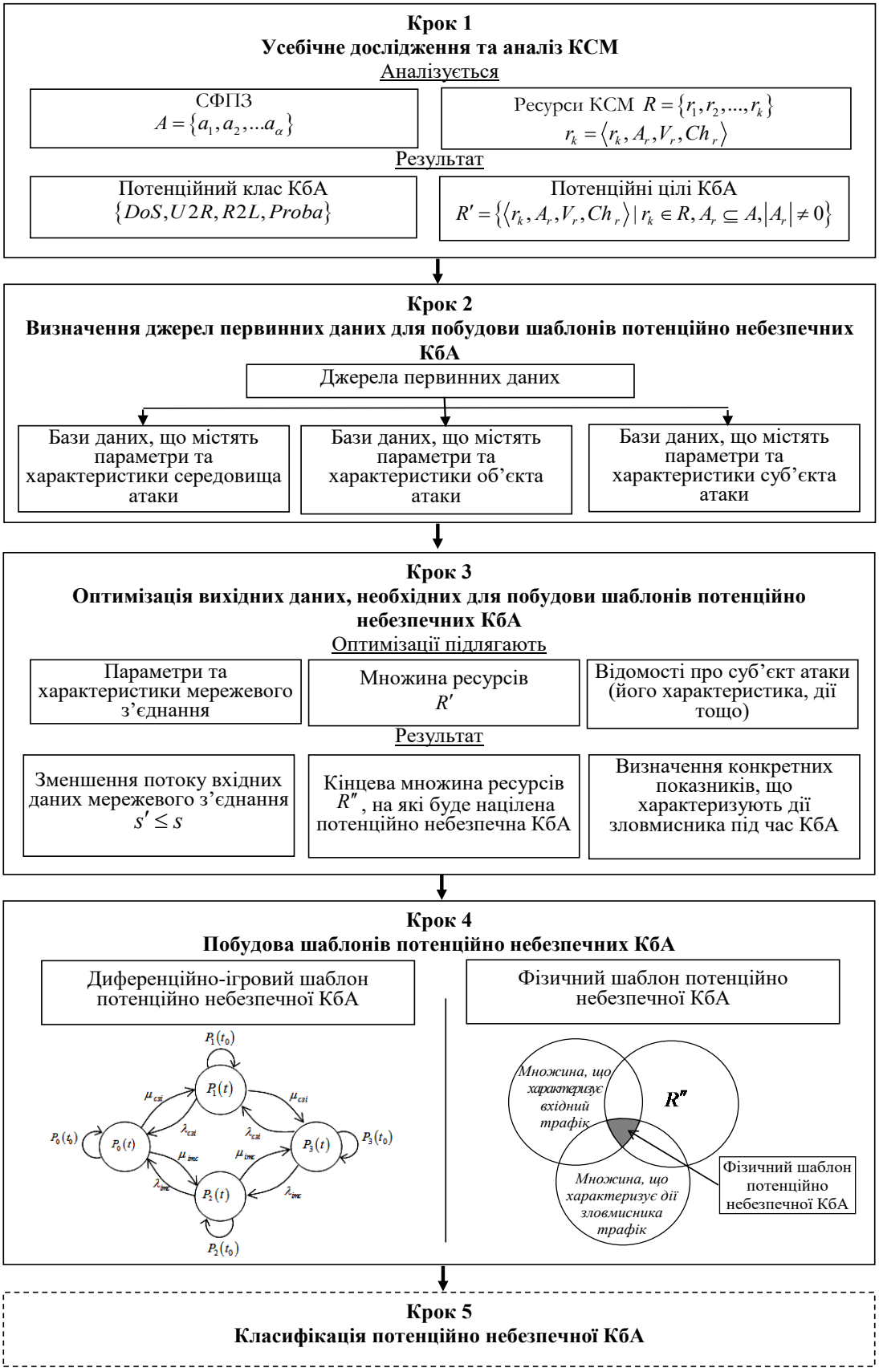

Рис 1. Структурна схема методу побудови шаблону потенційно небезпечної КбА

Висновки. Уперше запропоновано новий метод побудови шаблонів потенційно небезпечних КбА, який усуває базовий недолік відомих підходів – "ефект запізнення" в ході створення сигнатури. У його основу покладено визначення ключових характеристик

і параметрів потенційно небезпечної КбА, яке здійснюється на підставі аналізу стандартного функціонального профілю захищеності, реалізованого в КСМ, та джерел первинних даних, які використовуються для побудови шаблонів потенційно небезпечних КбА. У результаті практичного застосування зазначеного методу побудовано два шаблони потенційно небезпечної КбА на КСМ. Перший – диференційно-ігровий, який описує фізику процесів, що відбуваються в КСМ під час проведення потенційно небезпечної КбА. Другий – фізичний шаблон, який містить у собі повний набір характеристик та параметрів, властивих цій атаці.

Перспективним напрямом подальших досліджень є розроблення достовірної методики класифікації потенційно небезпечних КбА на КСМ.

СПИСОК ЛІТЕРАТУРИ

1. Geers K. Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn : CCDCOE, 2015. 176 c.
2. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах // Сучасна спеціальна техніка. 2011. № 1 (24). С. 61–66.
3. Олифер В. Г., Олифер Н. А. Безопасность компьютерных сетей. Москва : Горячая линия – Телеком, 2015. 644 с.
4. Звіт CERT-UA за 2010–2013 роки. URL: http://cert.gov.ua/?p=316 (дата звернення: 10.12.2019).
5. Киберщит Украины: кто стоит на страже кибергранниц страны. URL: http://zillya.ua/ru/kibershchit-ukrainy-kto-stoit-na-strazhe-kibergranits-strany (дата обращения: 23.12.2019).
6. Ларина Л., Овчинский В. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. Москва : Книжный мир, 2014. 352 с.
7. Lewis T. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. 2014. 400 p.
8. Ten C.-W. , Manimaran G., Liu C.-C. Cybersecurity for criticalinfrastructures: Attack and defense modeling // IEEETrans. Syst., Man Cybern. A. 2010. Vol. 40, No. 4. P. 853–865.
9. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность. Киев : Арий, 2008. 344 с.
10. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення. Київ : НАУ, 2011. 640 с.
11. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22–27.
12. Грищук Р. В. Диференціально-ігрова модель шаблону атаки на Web-сервер // Зб. наук. праць ВІКНУ ім. Т. Шевченка. 2010. № 21. С. 104–112.
13. Шабуров А. С. О разработке модели обнаружения компьютерных атак на объекты критической информационной инфраструктуры // Вестник ПНИПУ. 2018. № 26. С. 198–213.
14. НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу” [Затверджено наказом Адміністрації Держспецзв’язку від 15.10.2008 № 172]. 16 с.
15. Грищук Р., Охрімчук В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак // Безпека інформації. 2015. № 21 (3). С. 276–282.

16. Охрімчук В. Модель шаблону потенційно небезпечної кібератаки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техніч. зб. 2018. № 1 (35). С. 30–39.
17. Грищук Р. В., Охрімчук В. В., Ахтирцева В. С. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак // Захист інформації. 2016. № 1 (18). С. 21–29.
18. Khubeb Siddiqui M., Naahid S. Analysis of KDD CUP 99 Dataset using Clustering based Data Mining // International Journal of Database Theory and Application. 2013. Vol. 6, No. 5. P. 23–34.
19. Common Vulnerabilities and Exposures (CVE). URL: http://cve.mitre.org (last accessed: 10.12.2019).
20. Common Attack Pattern Enumeration and Classification. URL: https://capec.mitre.org. (last accessed: 15.12.2019).
21. UCI Knowledge Discovery in Databases Archive. URL: http://kdd.ics.uci.edu. (last accessed: 18.12.2019).
22. Грищук Р. В., Мамарєв В. М. Метод скорочення розмірності потоку вхідних даних для мережних систем виявлення атак // Сучасний захист інформації. Київ : ДУІКТ, 2012. Спецвипуск. С. 16–19.
23. Михалін Г. О., Дюженкова Л. І. Елементи теорії множин і теорії чисел. Київ : НПУ ім. М. П. Драгоманова, 2003. 128 с.
24. Пухов Г. Дифференциальные преобразования и математическое моделирование физических процессов : монография. Киев : Наук. думка, 1986. 160 с.
25. Грищук Р. Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію // Інформаційна безпека. 2009. № 2 (2). С. 128–132.
26. Классификация Ховарда. URL: http://helpiks.org/4-76231.html (дата обращения: 23.12.2019).
27. Корченко О. Г. Системи захисту інформації : монографія. Київ : НАУ, 2004. 264 с.
28. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения : монография. Киев : “МК-Пресс”, 2006. 320 с.
29. Классификация деструктивных информационных воздействий и кибератак. URL: http://antitentura.blogspot.com/2014/07/blog-post_11.html (дата обращения 23.12.2019).
30. Cyberattack classificator verification / V. Okhrimchuk, R. Hryshchuk, V. Mamarev et al. // Advances in Intelligent Systems and Computing. 2017. № 635. P. 402.

Подано 30.12.2019

В. В. Охримчук

МЕТОД ПОСТРОЕНИЯ ШАБЛОНОВ ПОТЕНЦИАЛЬНО ОПАСНЫХ КИБЕРАТАК

Сегодня в мире наблюдается существенное увеличение количества кибератак. При этом пропорционально возрастает их технологическая сложность. В ближайшем будущем не исключено появление новых потенциально опасных кибератак, что, в свою очередь, может привести к ухудшению их обнаружения и нейтрализации, а также, как следствие, негативно повлиять на уровень защищенности информационных и информационно-телекоммуникационных систем критической информационной инфраструктуры. С учетом изложенного в статье решается актуальная задача

разработки достоверного метода построения шаблонов потенциально опасных кибератак, внедрение которого обеспечит устранение базового недостатка создания сигнатур шаблонов атак, а именно "эффекта опоздания" по выработке нужной сигнатуры. В основу предложенного метода положено определение ключевых характеристик и параметров потенциально опасной кибератаки, которое осуществляется на базе анализа стандартного функционального профиля защищенности, реализованного в компьютерной системе и сети, а также источников первичных данных, которые используются для построения шаблонов потенциально опасных кибератак. Результатом практического применения данного метода является построение двух шаблонов потенциально опасной кибератаки на компьютерную систему и сеть. Первый – дифференциально-игровой шаблон потенциально опасной кибератаки, который описывает физику процессов, происходящих в компьютерной системе и сети во время проведения потенциально опасной кибератаки. Второй – физический шаблон, который включает в себя полный набор характеристик и параметров, характерных этой атаке.

Ключевые слова: *метод; уязвимость; кибератака; киберугроза; компьютерная система и сеть; система информационной безопасности; сигнатура; стандартный функциональный профиль защищенности; шаблон потенциально опасной кибератаки.*

V. V. Okhrimchuk

THE METHOD OF DEVELOPMENT A TEMPLATES OF POTENTIALLY DANGEROUS CYBER-ATTACKS

Today the world is experiencing a significant increase in the number of cyberattacks. At the same time, their technological complexity increases proportionally. In the near future, the emergence of new potentially dangerous cyberattacks is not ruled out, which in turn may lead to deterioration of their detection and neutralization and, consequently, negatively affect the level of security of information and information and telecommunications systems of critical information infrastructure. Based on this, the article solves the urgent problem of developing a reliable method of constructing patterns of potentially dangerous cyberattacks, the implementation of which eliminates the basic disadvantage of creating attack pattern signatures, namely the "delay effect" to produce the desired signature. The proposed method is based on the definition of key characteristics and parameters of a potentially dangerous cyber-attack. It is based on an analysis of the standard functional security profile implemented in the computer system and network and the primary data sources used to build the patterns of potentially dangerous cyberattacks. The practical application of this method will result in the construction of two patterns of potentially dangerous cyber-attack on a computer system and network. The first, a differential game template for a potentially dangerous cyberattack, will describe the physics of processes occurring in a computer system and network during a potentially dangerous cyberattack, and the second, a physical template, will contain the full set of characteristics and parameters inherent in that attack.

Keywords*: method; vulnerability; cyber-attack; cyber threat; computer system and network; information security system; signature; standard functional security profile; pattern of potentially dangerous cyber-attack.*