УДК 004.056.53

ДЖЕРЕЛА ПЕРВИННИХ ДАНИХ ДЛЯ РОЗРОБЛЕННЯ ШАБЛОНІВ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ КІБЕРАТАК

Руслан Грищук, Володимир Охрімчук, Влада Ахтирцева

Встановлено факт того, що ефективність функціонування сучасних систем забезпечення інформаційної та кібернетичної безпеки суттєво залежить від коректного та оперативного розроблення вендорами антивірусного програмного забезпечення шаблонів виявлених кібератак та своєчасного оновлення баз шаблонів атак цих систем користувачами послуг безпеки. Разом з тим постійне підвищення технологічної складності кібератак вимагає від вендорів постійного вдосконалення механізмів розроблення шаблонів кібератак. Одним із перспективних підходів вважається розроблення шаблонів потенційно небезпечних кібератак, тобто тих, які найімовірніше загрожуватимуть безпеці. Процедура розроблення таких шаблонів достатньо складна. Потреба забезпечення високої достовірності обумовлює необхідність урахування багатьох інформативних характеристик, які зможуть описати шаблон потенційно небезпечної кібератаки. Зокрема, це інформація про відомі шаблони кібератак та принципи їх побудови, вразливості та дефекти програмно-апаратних комплексів комп'ютерних систем й мереж, а також закладені в них розробником стандартні функціональні профілі захищеності та класифікатори кібератак. З цією метою у статті визначено перелік необхідних джерел, які запропоновано обрати як первинні дані для розроблення шаблонів потенційно небезпечних кібератак. Наведено їх порівняльні характеристики, проаналізовано переваги та недоліки. У результаті запропоновано узагальнену схему джерел первинних даних, яку покладено в основу розроблення шаблонів потенційно небезпечних кібератак. Показано, що перевагами обраних джерел первинних даних є те, що вендор має можливість визначити основні інформаційні складові шаблона потенційної небезпечної кібератаки ще до її прояву, тим самим збалансувавши дії сторін у системі інформаційного та кібернетичного протиборства.

Ключові слова: *база шаблонів кібератак, вразливість, кібератака, кіберзагроза, комп'ютерна система та мережа, сигнатура, стандартний функціональний профіль захищеності, шаблон потенційно небезпечної кібератаки.*

Вступ. З розвитком інформаційних технологій та впровадженням їх у всі сфери життя суспільства одним з найбільш пріоритетних напрямків наукових досліджень у галузі забезпечення інформаційної та кібернетичної безпеки є створення нових та дієвих методів, засобів виявлення кібератак (КбА) для захисту комп'ютерних систем та мереж (КСМ) державного та приватного секторів національної економіки. Постійне вдосконалення або модернізація діючих систем забезпечення інформаційної та кібернетичної безпеки (СЗ ІКБ) не може гарантувати повноцінного захисту КСМ від невідомих КбА [1–6]. З одного боку, це пов'язано зі збільшенням технологічної складності шкідливого програмного забезпечення (ШПЗ), а з іншого, – з існуванням основного недоліку технологічних процедур зі створення сигнатур шаблонів КбА, так званого "ефекту запізнення".

Таким чином, знаходження нових шляхів підвищення рівня захищеності КСМ залишається актуальною як науковою, так і практичною проблемою.

Аналіз останніх досліджень і публікацій [7–11] показав, що у світі існує достатньо велика кількість вендорів антивірусного програмного забезпечення, що займаються моніторингом, класифікацією та накопиченням відомостей про відомі кіберзагрози. Кожна така організація надає, як правило, відкритий доступ до своїх власних баз кіберзагроз. Але в різних вендорів та компаніях ці бази заповнюються різноманітною інформацією незалежно одна від одної. 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 призводить до нехтування рядом важливих інформативних характеристик, які описують КбА. Зокрема, нині не комплексуються між собою дані про існуючі шаблони КбА [12, 13], стандартні функціональні профілі захищеності (СФПЗ) [14, 15], класифікатори КбА[16–19], вразливості КСМ [20–21] тощо.

Метою статті є аналіз відомих й визначення з них найбільш інформативних джерел первинних даних, якими доцільно скористатися для розроблення шаблонів потенційно небезпечних КбА на КСМ.

Викладення основного матеріалу дослідження. Нехай множину відомих та загальнодоступних баз даних [9, 12, 13, 20, 21], що асоціюються фахівцями з інформаційної та кібернетичної безпеки як бази кіберзагроз, згрупуємо на основі принципів теорії подібності у вигляді трьох базових категорій (рис. 1).

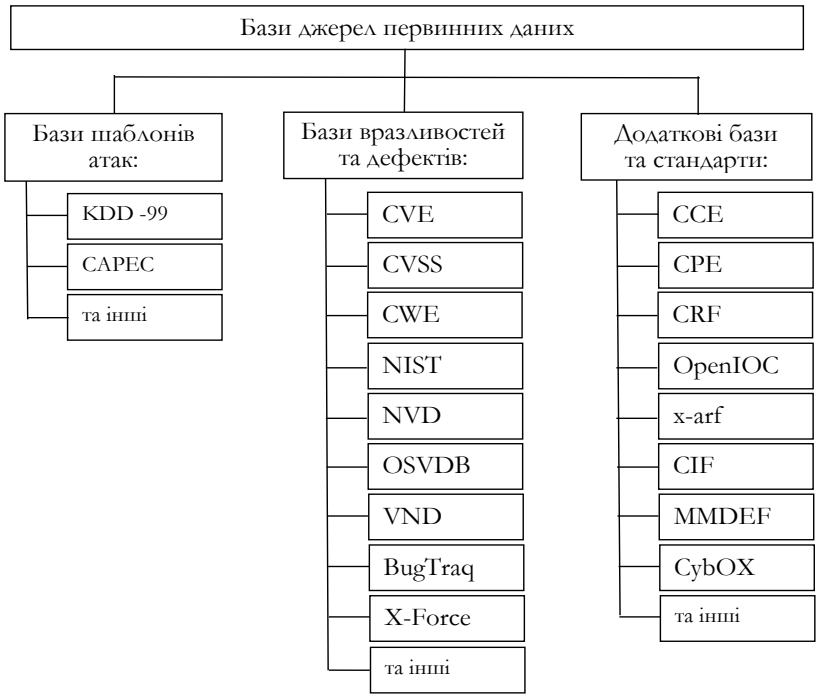


Рис. 1. Категорування баз даних на основі принципів теорії подібності

Усі існуючі бази кібернетичних загроз за інформацією, що зберігається в них, можна розділити на три великих категорії: бази шаблонів КбА, бази вразливостей та дефектів, інші додаткові бази та стандарти обміну даними про кіберзагрози (рис. 1).

Для подальшого дослідження й використання відомих баз як джерел первинних даних для розроблення шаблонів потенційно небезпечних КбА оберемо з них найбільш інформативні, починаючи з баз шаблонів КбА (див. рис. 1).

Нині як бази даних шаблонів КбА досить широко застосовуються бази KDD-99 та CAPEC. Проаналізуємо їх.

База шаблонів атак KDD-99 [22] містить $5 \cdot 10^6$ шаблонів мережевих з'єднань, які описують нормальну та аномальну поведінку трафіка в КСМ. Кожний шаблон складається з 41 параметра мережевого з'єднання (табл. 1) [22]. Як видно з табл. 1, параметри мережевого з'єднання групуються в окремі блоки – з першого по четвертий. Параметри запису *блока 1* являють собою основні характеристики TCP-з'єднання, зокрема, такі як тривалість, тип протоколу, кількість байтів від джерела/приймача. Параметри *блока 2* описують з'єднання на відомих для домена характеристиках і включають у себе кількість операцій створення файла, кількість невдалих спроб реєстрації тощо. І, нарешті, параметри *блока3* та *блока 4* належать до опису параметрів трафіка. Це величини, які обчислюються протягом часового інтервалу з дискретністю в 2 с. Причому, як показано в [23], *блок 3* відповідає часовим параметрам трафіка, *блок 4* – апаратним. Крім того, кожний шаблон у базі KDD-99 містить 42-е поле, яке вказує на стан трафіка в КСМ. Зазначене поле може набувати значення "*Normal*", якщо дане з'єднання належить до шаблона нормальної поведінки, або найменування типу КбА – *DoS, U2R, R2L, Probe*. Стан *"Normal"* передбачає відсутність загрози функціонуванню хоста КСМ. Згідно з [22] відомо, що нормальний стан роботи мережі поданий 972781 шаблонами, що у відсотковому значенні становить 19,8% від всього її об'єму. Решта шаблонів описують одну з чотирьох типів КбА (рис. 2).

Таблиця 1

Опис параметрів мережевого з'єднання за базою шаблонів атак KDD-99

	Блок 1				Блок 2		
	№ з/п	Назва показника	Опис	№ з/п	Назва показника	Опис
Базові характеристики TCP – з'єднання	1	Duration	Тривалість з'єднання	10	Hot	Кількість "гарячих" індикаторів, що вміщує контент, наприклад, проникнення до системних директорій, створення та виконання програм
	2	Protocol_ type	Протокол, що використовується при з'єднанні	11	Num_ failed_ logins	Кількість невдалих спроб авторизації
	3	Service	Цільовий сервіс, що використовується	12	Logged_ in	Статус авторизації: 1 – авторизація пройшла успішно, 0 – невдало
	4	Flag	Статус з'єднання: нормальне, помилка	13	Num_ compromised	Кількість скомпрометованих умов
	5	Src_bytes	Кількість байтів, переданих від джерела до приймача за одне з'єднання	14	Root_ shell	Дорівнює 1, якщо отримано права адміністратора, 0 – якщо ні
	6	Dst_bytes	Кількість байтів, переданих від приймача до джерела за одне з'єднання	15	Su_ attempted	Дорівнює 1, якщо була спроба отримати або отримано права адміністратора, 0 – якщо ні
	7	Land	Якщо джерело та приймач має однакові номери портів, то параметр набуває значення 1, якщо однакові – 0	16	Num_ root	Кількість адміністративного доступу, або кількість операцій, що виконуються від імені адміністратора в конкретному з'єднанні
	8	Wrong_ fragment	Загальна кількість пошкоджених фрагментів у конкретному з'єднанні	17	Num_file_cre-ations	Кількість операцій створення файлів в конкретному з'єднанні
	9	Urgent	Кількість термінових пакетів у конкретному з'єднанні. Терміновий пакет – це пакет, в якому активований біт терміновості URG	18	Num_ shells	Кількість запитів на надання доступу до оболонки адміністрування
				19	Num_ access_ files	Кількість операцій над файлом контролю доступу
				20	Num_out-bound_ cmds	Кількість вихідних команд у ftp сесії
				21	Is_hot_ login	Дорівнює 1, якщо авторизація належить "гарячому" списку, тобто адміністраторам, 0 – якщо ні
				22	Is_guest_ login	Дорівнює 1, якщо авторизація належить гостьовому запису, 0 – якщо ні
Параметри контенту						

	Блок 3				Блок 4		
	№ з/п	Назва показника	Опис	№ з/п	Назва показника	Опис
Часові параметри трафіка	23	Count	Кількість під'єднань до цільового хоста протягом часового інтервалу в 2 с.	32	Dst_host_ count	Кількість з'єднань з хостом
	24	Srv_ count	Кількість під'єднань до поточної служби (номеру порта) за останні 2 с.	33	Dst_host_ srv_count	Кількість з'єднань зі службою
	25	Serror_ rate	Відсоток з'єднань з помилкою типу SYN для даного хоста джерела	34	Dst_host_ same_srv_ rate	Відсоток з'єднань з даною службою на даному хості
	26	Srv_ serror_ rate	Відсоток з'єднань з помилкою типу SYN для даної служби джерела	35	Dst_host_ diff_srv_ rate	Відсоток з'єднань з різними службами на даному хості
	27	Rerror_ rate	Відсоток з'єднань з помилкою типу REJ для даного хоста джерела	36	Dst_host_ same_src_ port_rate	Відсоток з'єднання з даним хостом при поточному номері порта джерела
	28	Srv_ rerror_ rate	Відсоток з'єднань з помилкою типу REJ для даної служби джерела	37	Dst_host_ srv_diff_ host_rate	Відсоток з'єднань зі службою різних хостів
	29	Same_ srv_rate	Відсоток з'єднань зі службою	38	Dst_host_ serror_rate	Відсоток з'єднань з помилкою типу SYN для даного хоста приймача
	30	Diff_srv_ rate	Відсоток з'єднань з різними службами	39	Dst_host_ srv_ser-ror_rate	Відсоток з'єднань з помилкою типу SYN для даної служби приймача
	31	Srv_diff_ host_rate	Відсоток з'єднань з різними хостами	40	Dst_host_ rerror_rate	Відсоток з'єднань з помилкою типу REJ для даного хоста приймача
				41	Dst_host_ srv_rerror_ rate	Відсоток з'єднань з помилкою типу REJ для даної служби приймача
Апаратні параметри трафіка						

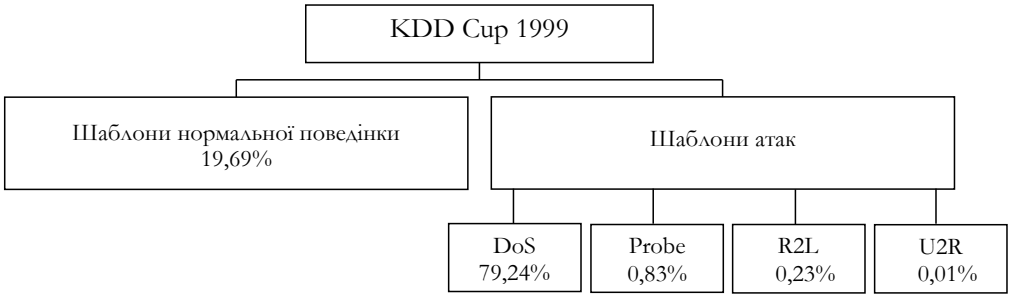


Рис. 2. Структура шаблонів нормальної поведінки та кібератак за базою *KDD Cup 1999*

Розглянемо шаблони КбА відповідно до даної бази (див. рис. 2).

Denial of Service Attack (DoS) – тип мережевої атаки, яка націлена на створення ситуацій, за яких КСМ, що атакується, відмовляє в обслуговуванні легальним користувачам. Даний тип КбА характеризується генерацією великого об'єму трафіка, що призводить до перевантаження серверного обладнання або комутаційних каналів. Наприклад, 24.08.2015 потужність КбА типу DDoS на сайті Міністерства закордонних справ України становила 3 – 5 Гбіт/с.

Users to Root Attack (U2R) – тип КбА, метою якої є отримання зареєстрованим користувачем привілеїв системного адміністратора (суперкористувача). Атаки даного типу, як правило, реалізуються інсайдерами.

Remote to Local Attack (R2L) – КбА, які спрямовані на отримання користувачем віддаленого несанкціонованого доступу до хоста. Одним з прикладів реалізації такого типу КбА є злам 22.05.2015 хакерським угрупованням "Кіберберкут" КСМ Міністерства фінансів України.

Probing Attack (Probe) – даний тип КбА направлений на одержання даних про КСМ для виявлення в ній незахищених профілів. Прикладом такої атаки є сканування портів, сніфінг тощо.

Аналіз рис. 2 показує, що одним із основних недоліків даної бази є недостатня кількість шаблонів КбА типу *U2R, R2L, Probe* (у цілому близько 1,07%), що у свою чергу, призводить до зниження ефективності використання її в локальних мережах, де ймовірність реалізації атак типу *DoS* малоймовірна. Крім того, наявні в базі записи не відображають алгоритм дій зловмисника, що може вплинути на можливість детектування модифікованої КбА.

Для більш ефективної побудови та використання СЗ ІКБ розробники шаблонів потенційно небезпечних КбА повинні знати алгоритми дій зловмисника при реалізації того чи іншого типу КбА. З цією метою можна скористатися відкритою базою шаблонів КбА CAPEC (Common Attack Pattern Enumeration and Classification) компанії MITRE [13].

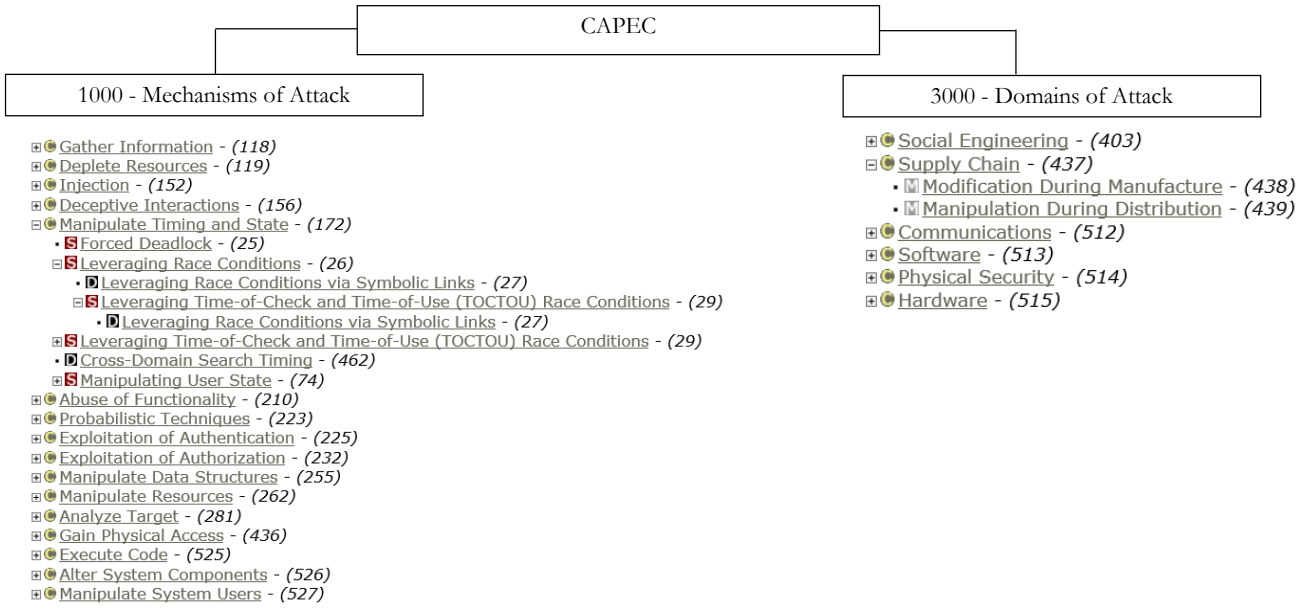
На сьогодні CAPEC – це складна ієрархічна структура сотень типів та видів КбА, які подані у текстовому вигляді. Всього база вміщує 504 шаблони КбА, які розподілені на два класи. Перший клас об'єднує шаблони КбА ієрархічно на основі механізмів, які найімовірніше використовують при експлуатації вразливості [24]. Категорії, які є членами цього класу, описують різні методи, що використовуються для КбА на КСМ але, як недолік, не відображають наслідків або цілей атаки (рис. 3а).

Другий клас ієрархії шаблонів КбА ґрунтується на цільовій сфері їх застосування (рис. 3а). Таким чином, як показав аналіз ієрархії шаблонів КбА за базою CAPEC, можна зробити висновок, що всі шаблони незалежно від класу поділені на категорії, які, у свою чергу, складаються з різних рівнів деталізації шаблонів КбА (рис. 3б).

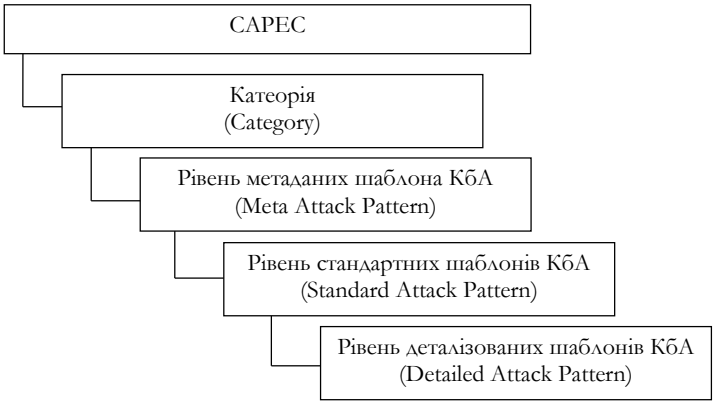
Категорія в CAPEC – це набір шаблонів КбА, об'єднаних на основі узагальнених характеристик – критеріїв [13].

Рівень метаданих шаблонів КбА в CAPEC (див. рис. 3б) – це абстрактний опис специфічної методології або способу, що використовується в КбА. Метадані шаблонів КбА здебільшого позбавлені певної технології або реалізації атаки і призначені для забезпечення розуміння сукупності підходів вищого рівня. Рівень метаданих шаблонів КбА є узагальненням відповідних груп стандартних шаблонів КбА. Рівень метаданих шаблонів КбА також ефективно використовується для моделювання кіберзагроз.

Рівень стандартних шаблонів КбА в CAPEC орієнтований на конкретну методологію або техніку, що використовується для проведення КбА. Як правило, він описує окремі частини повної КбА, що проводиться. Стандартні шаблони КбА призначені для забезпечення розробників додатковою інформацією для встановлення сутності технології досягнення бажаної мети КбА. Рівень стандартних шаблонів КбА є більш специфічним типом, на відміну від рівня метаданих шаблонів атак, який більш абстрактний.



а)



б)

Рис. 3. Структура бази CAPEC: а) загальна; б) ієрархічна.

Рівень деталізованих шаблонів КбА в CAPEC забезпечує низьку деталізацію КбА і, як правило, відображає використання конкретного методу та конкретних цілей, яких прагне досягти зловмисник внаслідок її реалізації. Деталізовані шаблони атак більш конкретні, ніж метадані шаблонів КбА та стандартні шаблони КбА, і переважно потребують використання специфічного механізму захисту для мінімізації наслідків КбА. Їм необхідне доповнення різними стандартними шаблонами КбА, об'єднаними разом для досягнення мети КбА.

Основна особливість CAPEC порівняно з іншими базами шаблонів атак полягає в тому, що в ній описують не окремі вразливості та критичні місця, а підходи та методики, що використовуються зловмисником для проведення КбА на КСМ. Разом з тим, основним недоліком CAPEC є відсутність у шаблонах КбА інформації про параметри мережевого з'єднання, стану вузла, що атакується, реакції КСМ на КбА.

У результаті аналізу й дослідження переваг та недоліків розглянутих вище баз встановлено, що для розроблення шаблона потенційно небезпечної КбА, який буде одночасно відображати як дії зловмисника, так і параметри мережевого з'єднання, необхідно скористатися принципом комплексування баз KDD-99 та CAPEC, взявши з кожної з них їх переваги та взаємокомпенсувавши недоліки.

Невід'ємними джерелами первинних даних для розроблення шаблонів потенційно небезпечних КбА також мають бути відомості про СФПЗ конкретної КСМ та класифікатор КбА. Знання СФПЗ КСМ дозволяє виявити її найменш та найбільш захищені компоненти.

Для доповнення обраних вище джерел первинних даних також доцільно скористатися СФПЗ, описаними в нормативному документі системи технічного захисту інформації НД ТЗІ 2.5–005–99. СФПЗ – це перелік мінімально необхідних рівнів послуг, які повинен реалізовувати комплекс засобів захисту інформації КСМ, щоб відповідати визначеним вимогам щодо захищеності інформації, яка обробляється в даній КСМ.

Відомо, що СФПЗ розробляються для КСМ на підставі відповідності встановленим вимогам із захисту інформації від загроз і відомих на сьогодні функціональних послуг, що дозволяють протистояти даним загрозам і забезпечують виконання поставлених вимог.

Функціональні послуги в НД ТЗІ 2.5–005–99 розбиті на чотири групи: конфіденційності, доступності, цілісності та спостережності. Кожна з груп критеріїв включає в себе послуги, що направлені на забезпечення кіберзахисту від відповідних загроз. Всього визначено 22 послуги. Схему критеріїв, назву та зміст послуг наведено в [14]. Кожна послуга являє собою набір функцій, метою яких є протистояння визначеній множині загроз. Як відомо, послуга може включати декілька рівнів. Чим вищий рівень послуги, тим більш повно вона забезпечує захист від певного виду загроз. Послуги різних видів та рівнів, що об'єднані між собою, формують СФПЗ КСМ. Відповідно до [15] профіль – це мінімально необхідний перелік послуг, який може забезпечити СЗІ, щоб відповідати певним вимогам щодо рівня захищеності від КбА в КСМ. Всього на сьогодні визначено 90 СФПЗ. Таким чином, можна стверджувати, що врахування СФПЗ при розробленні шаблонів потенційно небезпечних КбА забезпечить розробнику можливість визначення вектора потенційної КбА.

Також описані вище джерела не будуть повними, якщо їх не доповнити класифікаторами КбА. На сьогодні відомо багато різних підходів до класифікації КбА [16 – 19]. З аналізу [9] навіть вендори не мають єдиного бачення на класифікацію. Більшість відомих класифікаторів має досить умовний характер, що не дозволяє підійти системно до визначення належності КбА до того чи іншого класу згідно з KDD-99. Вважається, що найбільш повною та систематизованою класифікацією КбА, що використовується на практиці для вирішення ряду прикладних завдань, є узагальнена класифікація КбА, розроблена в [17] та подана в формалізованому вигляді в [25]. Перевагою обраного підходу до узагальненої класифікації КбА є застосування ознакового принципу для опису різних класів КбА. На відміну від відомих підходів до побудови класифікацій, ознаковий принцип забезпечує опис не тільки відомих на сьогодні класів КбА, а й дозволяє розширювати ознаковий простір для опису нових невідомих, і, відповідно, потенційно небезпечних класів.

Таким чином, оцінивши критично відомі бази (див. рис. 1) у загальному вигляді схему використання джерел первинних даних та комплексування інформації з них для розроблення шаблонів потенційно небезпечних КбА можна подати у вигляді узагальненої схеми (рис. 4).

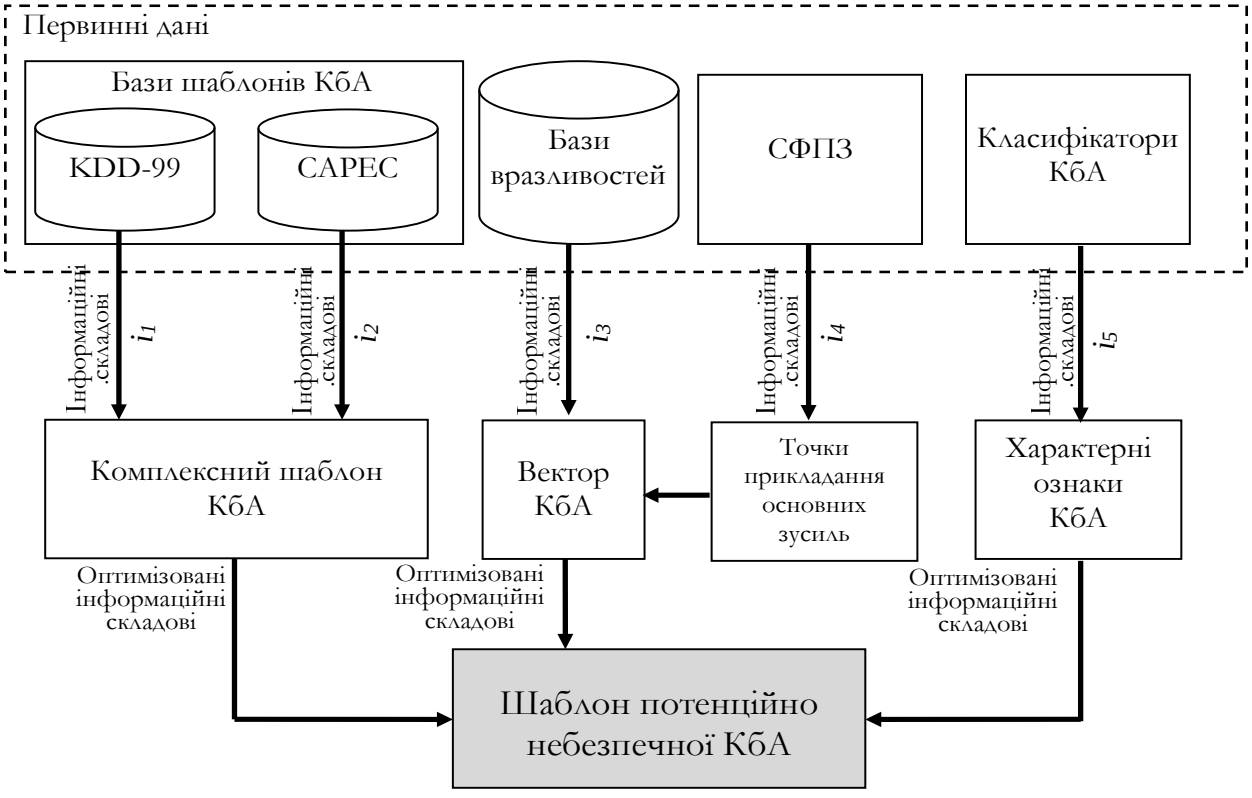


Рис. 4. Узагальнена схема формування джерел первинних даних для розроблення шаблонів потенційно небезпечних КбА

ЛІТЕРАТУРА

[1]. Олифер, В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. – М. : Горячая линия – Телеком, 2015. – 644 с.

[2]. Грищук, Р. В. Атаки на інформацію в інформаційно-комунікаційних системах / Р. В. Грищук // Сучасна спеціальна техніка – 2011. – №1(24). – С.61-66.

[3]. Звіт CERT-UA за 2010-2013 роки [Електронний ресурс]. – 2014. – Режим доступу до ресурсу : http://cert.gov.ua/?p=316.

[4]. Ларина, Л. Кибервойны XXI века. О чем умолчал Эдвард Сноуден / Л. Ларина, В. Овчинский. – М. : Книжный мир, 2014. – 352 с.

[5]. Бурячок, В. Л. Політика інформаційної безпеки / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко ; під заг. ред. проф. В. О. Хорошка. – К.: ПВП «Задруга», 2014. – 222 с.

[6]. Check Point: 84% компаний загружают вредоносное ПО каждые 10 минут [Електронний ресурс] // Check Point Software Technologies. – 2015. – Режим доступу до ресурсу: http://servernews.ru/820500.

[7]. Касперський, Є. Про Kaspersky Lab [Електронний ресурс] / Є. Касперський // http://www.kaspersky.ua/about#. – 2015.

[8]. 8000000-й вирус добавлен в вирусные базы Zillya! [Електронний ресурс] // Zillya!. – 2013. – Режим доступу до ресурсу : http://zillya.ua/ru/8000000-i-virus-dobavlen-v-virusnye-bazy-zillya.

[9]. Котенко, И. В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей / И. В. Котенко, А. А. Чечулин, А. В. Федорченко. // Информационно-управляющие системы. – 2014. – №5. – С. 72–79.

[10]. Лучший антивирус 2015 [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: http://remontka.pro/best-antivirus-2015/.

[11]. [Антивирус Nod32: достоинства, недостатки и особенности работы [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: http://sysc.ru/blog/antivirus-nod32-dostoinstva-nedostatki-i-osobennosti-raboty/.

[12]. Shrivas A. K. An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set / A. K. Shrivas, A. K. Dewangan // International Journal of Computer Applications. – 2014. – Volю 99, № 15. – P. 8–13.

[13]. Офіційний сайт Common Attack Pattern Enumeration and Classification [Електронний ресурс] – Режим доступу до ресурсу: https://capec.mitre.org.

[14]. НД ТЗІ 2.5-005-99 " Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

[15]. НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".

[16]. Классификация Ховарда [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: http://helpiks.org/4-76231.html.

[17]. Корченко О. Г. Системи захисту інформації : монографія / О. Г. Корченко. – К. : НАУ, 2004. – 264 с.

[18]. Корченко, А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения : монография /Корченко А. Г. – К. : "МК-Пресс", 2006. – 320с.

[19]. Классификация деструктивных информационных воздействий и кибератак [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://antitentura.blogspot.com/2014/07/blog-post_11.html.

[20]. Офіційний сайт Common Vulnerabilities and Exposures (CVE) [Електронний ресурс] – Режим доступу до ресурсу: http://cve.mitre.org.

[21]. Банк данных угроз безопасности информации [Електронний ресурс] – Режим доступу до ресурса: http://www.bdu.fstec.ru/threat.

[22]. Khubeb Siddiqui M. Analysis of KDD CUP 99 Dataset using Clustering based Data Mining / M. Khubeb Siddiqui, S. Naahid. // International Journal of Database Theory and Application. – 2013. – С. pp.23–34.

[23]. Мамарєв, В. В. Метод побудови класифікатора кібератак на державні інформаційні ресурси : дис. канд. техн. наук : 21.05.01 / Мамарєв В. В. – Київ, 2015. – 160 с.

[24]. Котенко, И. В. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения / И. В. Котенко. // Защита информации. Инсайд.. – 2012. – №4. – С. 54–66.

[25]. Грищук, Р. В. Диференціально-ігрові моделі та методи моделювання процесів кібернападу : автореф. дис. на здобуття наук. ступеня докт. техн. наук : спец. 21.05.01 / Грищук Р. В. – Київ, 2013. – 40 с.

REFERENCES

[1]. Olifer V. H. Computer Network Security / V. H. Olifer, N. A. Olifer. – M. : Hot line – Telecom, 2015. – 644 p.

[2]. Hryshchuk, R. V. Attacks on information in the information and communication systems / R. V. Hryshchuk // Modern special technique – 2011. – No 1(24). – pp.61-66.

[3]. Report of CERT-UA for the years 2010-2013 [Electronic resource]. – 2014. – Access to resources: http://cert.gov.ua/?p=316.

[4]. Larina, L. Cyber war of the XXI century. What silent Edward Snowden / L. Larina, V. Ovchinskii. – M. : Knizhnyi mir, 2014. – 352 p.
[5]. Buriachok, V. L. Information security policy / V. L. Buriachok, R. V. Hryshchuk, V. O. Khoroshko. – K. : PVP "Zadruga", 2014. – 222 p.
[6]. Check Point: 84% of companies charged with malware every 10 minutes [Electronic resource]. // Check Point Software Technologies. – 2015. – Access to resources: http://servernews.ru/820500.
[7]. Kasperskii, E. About Kaspersky Lab [Electronic resource]. – 2015. – Access to resources : http://www.kaspersky.ua/about#.
[8]. 8000000 th virus added to the virus database Zillya! [Electronic resource]. – 2015. – Access to resources : http://zillya.ua/ru/8000000-i-virus-dobavlen-v-virusnye-bazy-zillya.
[9]. Kotenko, I. V. Researching of the open database of vulnerabilities and assessment of the possibility their application in network security analysis of computer systems / I. V. Kotenko, A. A. Chechulin, A. V. Fedorchenko. // Information Control Systems. – 2014. – No. 5. – pp. 72–79.
[10]. The best antivirus 2015 [Electronic resource]. – 2015. – Access to resources: http://remontka.pro/best-antivirus-2015/.
[11]. Antivirus Nod32: advantages, disadvantages and features of work [Electronic resource]. – 2015. – Access to resources: http://sysc.ru/blog/antivirus-nod32-dostoinstva-nedostatki-i-osobennosti-raboty/.
[12]. Shrivas A. K. An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set / A. K. Shrivas, A. K. Dewangan // International Journal of Computer Applications. – 2014. – Volю 99, № 15. – P. 8–13.
[13]. Official site Common Attack Pattern Enumeration and Classification [Electronic resource]. – 2015. – Access to resources: https://capec.mitre.org.
[14]. ND Technical information protection 2.5-005-99 " Criteria for evaluating of information security in computer systems from unauthorized access ".
[15]. ND Technical information protection 2.5-005-99 " Classification of of the automated systems and standard functional profiles of protection information processed from unauthorized access ".
[16]. Classification of Howard [Electronic resource]. – 2015. – Access to resources: http://helpiks.org/4-76231.html.
[17]. Korchenko, A. H. Information protection systems: monograph / A. H. Korchenko. – K. : NAU, 2004. – 264 p.
[18]. Korchenko, A. H.. Building of the information protection systems on fuzzy sets. Theory and practical solutions: a monograph / A. H. Korchenko – K. : "MK-Press", 2006. – 320 p.
[19]. Classification of the destructive information impacts and cyber-attacks [Electronic resource]. – 2014. – Access to resources : http://antitentura.blogspot.com/2014/07/blog-post_11.html.
[20]. Official site Common Vulnerabilities and Exposures (CVE) [Electronic resource]. – 2015. – Access to resources: http://cve.mitre.org.
[21]. Data bank of Information security threats [Electronic resource]. – 2015. – Access to resources: http://www.bdu.fstec.ru/threat.
[22]. Khubeb Siddiqui M. Analysis of KDD CUP 99 Dataset using Clustering based Data Mining / M. Khubeb Siddiqui, S. Naahid. // International Journal of Database Theory and Application. – 2013. – C. pp.23–34.
[23]. Mamaryev, V. V. Method of constructing classifier of cyber attacks on governmental information resources: dis. Ph.D.: 21.05.01 / Mamaryev V. V. – Kiev, 2015. – 160 p.
[24]. Kotenko, I. V. Common Attack Pattern Enumeration and Classification (CAPEC): description and application examples / I. V. Kotenko. // Information protection. Inside. – 2012. – No. 4. – pp. 54–66.
[25]. Hryshchuk, R. V. Differential-game models and methods of modeling processes of cyber attacks: Manuscript Dr. of Techn. Sci. / Hryshchuk R. V. – Kiev, 2013. – 40 p.

ИСТОЧНИКИ ПЕРВИЧНЫХ ДАННЫХ ДЛЯ РАЗРАБОТКИ ШАБЛОНОВ ПОТЕНЦИАЛЬНО ОПАСНЫХ КИБЕРАТАК

Установлен факт того, что эффективность функционирования современных систем обеспечения информационной и кибернетической безопасности существенно зависит от корректной и оперативной разработки вендорами антивирусного программного обеспечения шаблонов выявленных кибератак и своевременного обновления баз шаблонов атак этих систем пользователями услуг безопасности. Вместе с тем, постоянное повышение технологической сложности кибератак требует от вендоров постоянного совершенствования механизмов разработки шаблонов кибератак. Одним из перспективных подходов считается разработка шаблонов потенциально опасных кибератак, то есть тех из них, которые вероятнее всего будут угрожать безопасности. Процедура разработки таких шаблонов достаточно сложная. Потребность обеспечения высокой достоверности обусловливает необходимость учета многих информативных характеристик, которые смогут описать шаблон потенциально опасной кибератаки. В частности, это информация об

известных шаблонах кибератак и принципов их построения, уязвимости и дефекты программно-аппаратных комплексов компьютерных систем и сетей, а также заложенные в них разработчиком стандартные функциональные профили защищенности и классификаторы кибератак. С этой целью в статье определен перечень необходимых источников, которые предложено избрать как первичные данные для разработки шаблонов потенциально опасных кибератак. Приведены их сравнительные характеристики, проанализированы преимущества и недостатки. В результате предложено обобщенную схему источников первичных данных, которая положена в основу разработки шаблонов потенциально опасных кибератак. Показано, что преимуществами выбранных источников первичных данных является то, что вендор имеет возможность определить основные информационные составляющие шаблона потенциальной опасной кибератаки еще до ее проявления, тем самым сбалансировав действия сторон в системе информационного и кибернетического противоборства.

Ключевые слова: база шаблонов кибератак, уязвимость, кибератака, киберугроза, компьютерная система и сеть, сигнатура, стандартный функциональный профиль защищённости.

THE SOURCES OF PRIMARY DATA FOR THE DEVELOPMENT POTENTIALLY DANGEROUS PATTERNS OF CYBER-ATTACKS

It was established fact that the efficiency of modern systems of information and cyber security essentially depends on correct and timely development by vendors of antivirus software patterns of the detected cyber-attacks and timely update databases pattern of attacks these users of security. However, the constant improvement of the technological complexity of cyber-attacks requires from vendors constant improvement of mechanisms of development patterns of cyber-attacks. One of the promising of approaches is considered a developing pattern of potentially dangerous cyberattacks, that of those who are likely to threaten security. The procedure for development of such patterns is enough complicated. The need for providing high of authenticity necessitates consideration of many informative characteristics which will be able describe the pattern of potentially dangerous cyber-attacks. In particular, this information about known patterns of cyber-attacks and the principles of their construction, vulnerabilities and defects of software and hardware complexes of computer systems and networks, and in them the developer of standard functional profiles of protection, classifiers of cyber-attacks. For this purpose, the article defines the list necessary sources that asked to choose a primary data for the development of potentially dangerous patterns of cyber-attacks. Shown of their comparative characteristics, analyzed advantages and disadvantages. As a result, the proposed the generalized scheme of primary data sources, which is the basis of development potentially dangerous patterns of cyber-attacks. Shown that the benefits of the selected sources of primary data is that the vendor has the opportunity to identify the main information components of potentially dangerous pattern of cyber-attacks even before its manifestation thereby balancing actions of the parties in the system of information and cyber confrontation.

Keywords: database pattern of cyber-attacks, vulnerability, cyber-attack, cyberthreats, computer system and network, signature, standard functional profile of protection, potentially dangerous patterns of cyber-attacks.

Грищук Руслан Валентинович, доктор технічних наук, старший науковий співробітник, начальник науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова
E-mail: Dr.Hry@i.ua

Грищук Руслан Валентинович, доктор технических наук, старший научный сотрудник, начальник научно-исследовательского отдела информационной и кибернетической безопасности научного центра Житомирского военного института имени С. П. Королёва.

Hryshchuk Ruslan, Dr. of Techn. Sci., Senior Researcher, Chief of Scientific Research Department Information and Cybersecurity of Scientific Center of Zhytomyr Military Institute after S. P. Korolyov.

Охрімчук Володимир Васильович, науковий співробітник науково-дослідної лабораторії проблем забезпечення кібернетичної безпеки наукового центру Житомирського військового інституту імені С. П. Корольова.
E-mail: Okhrimchuk84@ukr.net

Охримчук Владимир Васильевич, научный сотрудник научно-исследовательской лаборатории проблем кибернетической безопасности научного центра Житомирского военного института имени С. П. Королёва.

Okhrimchuk Vladimir, research scientist of scientific research laboratory issues of cybersecurity of scientific center of Zhytomyr military institute after S. P. Korolyov.

Ахтирцева Влада Сергіївна, офіцер в/ч А1912.
E-mail: perri92@i.ua

Ахтырцева Влада Сергеевна, офицер в/ч А1912.

Akhtyrtseva Vlada, an officer of the military unit A 1912**.**