DOI:
УДК 004.056

Ю. Л. Поночовний, кандидат технічних наук, старший науковий співробітник, доцент кафедри інформаційних систем та технологій Полтавської державної аграрної академії
С. Ю. Рогочий, магістр Полтавського національного технічного університету імені Юрія Кондратюка
О. І. Шарай, магістр Полтавського національного технічного університету імені Юрія Кондратюка
В. О. Кнуренко, магістр Полтавського національного технічного університету імені Юрія Кондратюка
В. С. Воронянський, викладач Полтавського коледжу нафти і газу Полтавського національного технічного університету імені Юрія Кондратюка

ДОСЛІДЖЕННЯ БАЗ ВРАЗЛИВОСТЕЙ ДЛЯ ПАРАМЕТРИЗАЦІЇ МАРКОВСЬКИХ МОДЕЛЕЙ ОЦІНЮВАННЯ ДОСТУПНОСТІ ВЕБ-РЕСУРСІВ

Досліджено актуальне питання оцінювання параметрів вразливостей веб-ресурсів для використання як вхідних даних у марковських моделях доступності. Наведено розрахунки інтенсивності прояву вразливостей доступності веб-серверів сімейства Apache на основі вибірок за 2015 та 2016 рр. У статті розглянуто зв'язки між базами вразливостей, зокрема між базою CVE та іншими відкритими та платними репозитаріями. Основна увага приділяється питанням актуалізації наведеної у відкритих базах інформації, уточненню часу фіксації вразливості в базі та формуванню вибірок на основі множини критеріїв відбору.

Ключові слова: *вразливості веб-ресурсів; оцінювання параметрів; інтенсивність прояву; критичність вразливості.*

© Ю. Л. Поночовний, С. Ю. Рогочий, О. І. Шарай, В. О. Кнуренко, В. С. Воронянський, 2019

Рассмотрены актуальные вопросы оценки параметров уязвимостей веб-ресурсов для использования в качестве входных данных в марковских моделях доступности. Приведены расчеты интенсивности проявления уяз вимостей доступности веб-серверов семейства Apache на основе выборок за 2015 и 2016 гг. В статье рассматриваются связи между базами уязви-мостей, в частности, между базой CVE и другими открытыми и платны-ми репозитариями. Основное внимание уделяется вопросам актуализации приведенной в открытых базах информации, уточнению времени фиксации уязвимости в базе и формированию выборок на основе множества крите-риев отбора.

Ключевые слова: *уязвимости веб-ресурсов; оценивание параметров; ин-тенсивность проявления; критичность уязвимости.*

In this paper we consider issues of obtaining information from open data-bases of vulnerabilities and the creation of excerpt according to several criteria. The relevance of the topic is due to the need to ensure the parameterization of samples. Simulation helps increase the likelihood of detecting a vulnerability be-fore it is used by attackers. The issues of assessing the parameters of vulnerabili-ties of web resources are considered. These parameters are used as input in Mar-kov availability models. Availability is included in the set components of infor-mation security (confidentiality, integrity, availability).

The article discusses the relationship between databases of vulnerabilities. The relationships between the CVE database and other open and paid reposito-ries are analyzed. Analyzed the current state of relations (uplink or downlink). The focus is on issues of updating the information given in open databases. The activity of the database, their openness, paid access or the possibility of trial / limited use are determined.

For processing, information from the NVD vulnerability database in the form of archived XML files was obtained and refined. The following parameters were used as input parameters for Markov models: the intensity of the manifesta-tion of vulnerabilities and the criticality of the attack. The calculations of the in-tensity of the availability of vulnerabilities of Apache family of web servers based on samples for 2015 and 2016 are given. Attention is paid to the specification of the time of fixation of vulnerabilities in the database and the formation of samples based on a set of selection criteria from the open bases of vulnerabilities of NVD and CVE.

The results of the study showed that in 2016, new vulnerabilities from the sample were recorded 3.23 times faster, but at the same time, their criticality de-creased by 3 % on average. The tendency of gradual growth of interest to net-work software products, in particular Apache web servers, is confirmed.

To speed up and more convenient excerpt creation, it is advisable to develop software that automatically creates the necessary excerpte after selecting the formation criteria. Also, to improve the results of the study, it is necessary to refine the vulnerability information in several open bases.

Key words: *vulnerability of web resources; parameter estimation; intensity of manifestation, critical score.*

Постановка проблеми. За останні десятиліття залежність сучасного суспільства від комп'ютерних систем істотно зросла. Банківські операції, управління торгівлею ринків, автоматизовані військові й державні системи все більше залежать від комп'ютерних систем. У результаті ризик реалізації різних класів атак, які базуються на експлуатації наявних вразливостей у програмно-апаратному забезпеченні, для критично важливих об'єктів дуже великий [1].

Як наслідок, в наші дні проводяться великомасштабні дослідження проблем безпеки та кібербезпеки, викликаних уразливостями програмно-апаратного забезпечення [2]. Незважаючи на наявні загрози, суспільство вже ніколи не відмовиться від використання мережі Інтернет і комп'ютерних мереж в цілому, адже вони дають величезні можливості у фінансовій, політичній, військовій та інших галузях. Постійне вдосконалення технологій безпеки в інформаційному світі не може гарантувати абсолютну захищеність комп'ютерних систем.

Вразливості виявлялись у всіх основних операційних системах і додатках. Так як постійно знаходять нові вразливості, єдиний шлях зменшити ймовірність їх використання зловмисниками полягає у виконанні безперервного моніторингу захищеності, що передбачає постійне відстеження появи вразливостей, оперативне встановлення оновлень та використання інструментів протидії можливим атакам.

Наприклад, вразливість операційної системи може призвести до витоку комерційної інформації, що спричинить значні фінансові втрати. У таких умовах корисно було б мати змогу оцінювати, прогнозувати безпеку комп'ютерної системи, її компонентів, локальних і веб-ресурсів. Одним зі способів прогнозування безпеки є моделювання процесів виявлення й усунення вразливостей на основі статистичних даних, зібраних за певний період життєвого циклу (далі – ЖЦ) програмних засобів.

Аналіз останніх досліджень і публікацій. Із кожним роком спостерігається підвищення зацікавленості науковців і незалежних дослідників-ентузіастів як до питання виявлення та занесення нових вразливостей до відомих БД, так і до використання доступної в БД інформації для оцінювання захищеності інформаційних систем і веб-ресурсів.

Нині існує цілий ряд інформаційних ресурсів Інтернет, які надають інформацію про вразливості на сторінках своїх сайтів. Одна з найвідоміших баз вразливостей – "Загальні вразливості та ризики" (Common Vulnerabilities and Exposures – CVE) компанії MITRE [3]. Базу CVE більшість дослідників вважає єдиним і первинним постачальником ідентифікаторів вразливостей. Ці ідентифікатори використовуються для однозначного позначення однієї й тієї ж уразливості іншими відомими базами даних (Secunia [4], Security Focus [4] та ін.), базами експлойтів (Exploit Database [6] тощо) і бюлетенями безпеки (Microsoft Security Bulletin [7], US-CERT [8], Android Security Bulletin [9] тощо). Недолік БД CVE – це відсутність в описі вразливостей специфікації програмно-апаратного забезпечення. Для визначення цієї специфікації потрібно використовувати першоджерела, які надали інформацію. Наприклад, база даних вразливостей NVD [10] дозволяє точно ідентифікувати вразливий програмний продукт та його версію, отримати інформацію про спосіб атаки, за якої дана вразливість виявляє себе, різновид загрози та іншу корисну інформацію.

У працях науковців досліджувались питання формування альтернативних (більш зручних) БД [11], використання інформації з БД вразливостей для побудови моделей захищеності [2; 12; 13]. На особливу увагу заслуговують дослідження ризиків, пов'язаних із віднаходженням та експлуатацією вразливостей веб-ресурсів. Такі дослідження можна умовно поділити на аналіз ризиків на основі статичних імовірнісних моделей [14] та дослідження зміни у часі показників захищеності систем, зокрема доступності, на основі динамічних марковських моделей [13; 15]. Питання параметризації динамічних моделей частково були розглянуті в [16; 17].

Мета статті – параметризація вразливостей на основі вибірок із відкритих баз даних. Для розв'язання задачі необхідно послідовно побудувати вибірку з бази, уточнити отримані дані та отримати кількісні оцінки.

Виклад основного матеріалу. Стан досліджень у питаннях інформаційної та кібербезпеки потребує адекватного уявлення ситуації сьогодення. Із часом виявляються нові вразливості у розробленому програмному забезпеченні, виходять нові версії програм, розробляють як експлойти (скрипти та програми для використання вразливостей), так і патчі, що усувають виявлені вразливості. Через певні причини (досить часто через фінансування) припиняють функціонування великі й малі проекти, що розробляють і супроводжують бази вразливостей. Нині щодо фінансування, наповнення та супроводу, а також підтримки взаємозв'язків опорною БД вразливостей є база CVE. Ця база підтримує взаємозв'язки з іншими репозитаріями, що відображено на відповідній сторінці ресурсу [18]. На момент написання статті нараховується 83 посилання на інші репозитарії, але, що важливо, деякі з них уже припинили підтримку проектів.

Під час дослідження джерел взаємозв'язків бази CVE було розглянуто бази даних із різними моделями доступу (рис. 1). Основними видами доступу є відкритий і закритий. Відкрита БД забезпечує доступ до даних про вразливості для користувачів без будь-яких обмежень. Доступ до даних у закритій базі неможливий без виконання певних умов, заданих власником БД (як правило, платний доступ).

Також існують закриті БД, що дають користувачеві обмежений, або навіть повний доступ на пробний період. Навпаки, деякі відкриті БД частково обмежують інформацію про вразливість. Такі способи доступу до БД не можна зараховувати до основних через тимчасовість/обмеженість такого доступу (на рис. 1 позначено БД із пробним періодом/обмеженим функціоналом).

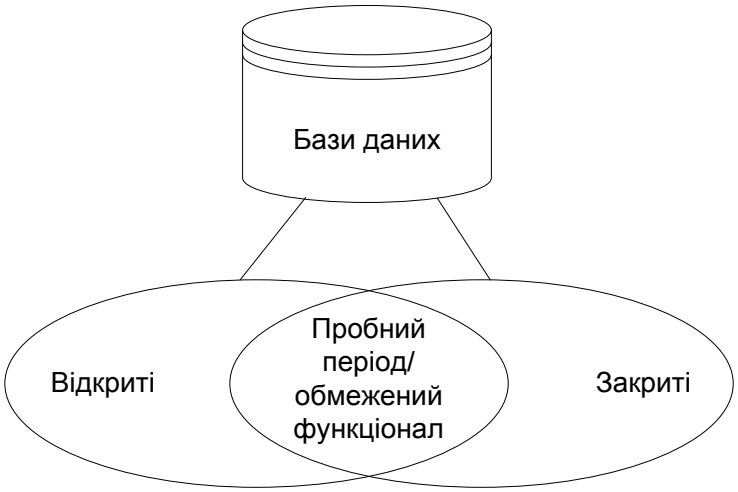

Рис. 1. Класифікація вразливостей БД за способом доступу

Репозитарії, відмічені у БД CVE, також можна розділити на групи (рис. 2) за характером контенту та його відношенням до певного об'єднувального фактора (найчастіше таким фактором є компанія–розробник програмного забезпечення). Універсальні БД не мають основного критерію для відбору вразливостей у свої бази; спеціалізовані БД мають єдину тему, що об'єднує інформацію про вразливості. Зі свого боку спеціалізовані поділяються на БД, в яких зібрані вразливості продуктів якогось одного виробника (загальні за виробником) та БД, які накопичують інформацію про вразливості одного типу продуктів різних виробників (спеціалізовані за продуктом).

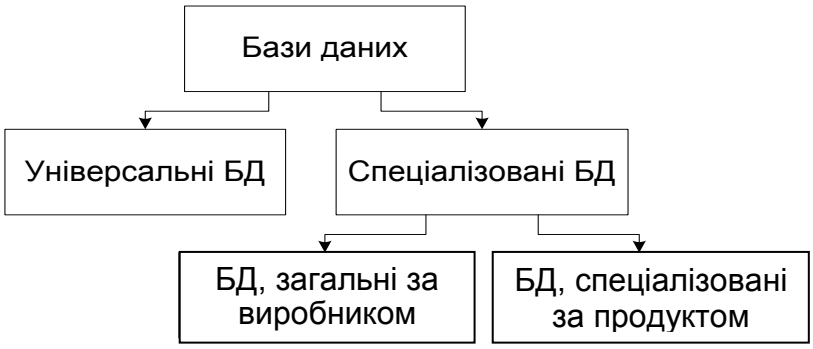

Рис. 2. Типізація вразливостей БД

Проект CVE розробила і підтримує компанія MITRE з 1999 р. На січень 2019 р. БД нараховує 143 934 записи (111 623, за даними веб-сайту). В табл. 1 відібрані БД, що були представлені у списку перехресних посилань бази CVE, та активні станом на кінець 2018 р. Головними причинами припинення роботи решти репозитаріїв стали банкрутство та реструктуризація компаній, що створили ці БД.

Таблиця 1

БД перехресних посилань бази CVE
(активні станом на кінець 2018 р.)

Назва	URL адреса	Тип
1	2	3
AIXAPAR	http://www-01.ibm.com/support/search.wss?rs=0&apar=only	закрита (безкоштовна 30-денна версія)
APPLE	http://lists.apple.com/archives/security-announce	відкрита
CERT	http://www.cert.org/advisories	відкрита
CERT-VN	http://www.kb.cert.org/vuls	відкрита
CHECKPOINT	http://www.checkpoint.com/defense/advisories/public/summary.html	відкрита
CISCO	http://www.cisco.com/en/US/products/products_security_advisories_listing.html	відкрита
CONECTIVA	http://lwn.net/Alerts/Conectiva/	відкрита
DEBIAN	http://www.debian.org/security/	відкрита
EXPLOIT-DB	http://www.exploit-db.com	відкрита
FEDORA	https://lists.fedoraproject.org/archives/list/announce@lists.fedoraproject.org/	відкрита

Закінчення табл. 1

1	2	3
FREEBSD	http://www.freebsd.org/security/	відкрита
GENTOO	http://www.gentoo.org/security/en/glsa/	відкрита
JVN	http://jvn.jp/en/report/index.html	відкрита
JVNDB	http://jvndb.jvn.jp/	відкрита
MANDRAKE	http://lwn.net/Alerts/Mandrake/	відкрита
MS	http://www.microsoft.com/technet/security/current.aspx	відкрита
NETBSD	http://www.netbsd.org/Security/advisory.html	відкрита
OPENBSD	http://www.openbsd.org/security.html	відкрита
REDHAT	http://www.redhat.com/support/errata/index.html	відкрита
SECTRACK	http://www.securitytracker.com	закрита (час пробної версії не зазначений)
SECUNIA	http://secunia.com/advisories/	відкрита
SLACKWARE	http://www.slackware.com/security/	відкрита
SREASON	http://securityreason.com/security_alert	відкрита
SUSE	https://www.suse.com/support/update/	відкрита
TURBO	http://www.turbolinux.com/security/	відкрита
UBUNTU	http://www.ubuntu.com/usn/	відкрита
VIM	http://www.attrition.org/pipermail/vim/	відкрита
XF	https://exchange.xforce.ibmcloud.com/	закрита (безкоштовна 30-денна версія)

Формування вибірки для оцінювання вхідних параметрів марковських моделей доступності

Як вхідні параметри марковських моделей оцінювання доступності може бути використано інтенсивність вияву вразливостей та критичність атаки [17]. Для оцінювання середнього значення інтенсивності вияву вразливостей при допущеннях, зазначених у [16], можливо використання часових міток – часу фіксації вразливості в БД (якщо вразливість зафіксовано в різних репозитаріях, необхідно визначити найраніший час внесення вразливості в БД).

Дослідження дат, що містяться в файлах форматів CVE, CVRF і NVD, показують, що публікація однієї й тієї ж вразливості в NVD відбувається значно пізніше (як правило, через кілька тижнів, а іноді й місяців), ніж у CVE або CVRF. Даний факт може свідчити про те, що фахівцям, які супроводжують базу NVD, потрібно більше часу перед публікацією інформації

про вразливість, щоб зібрати більше інформації про неї (метрики критичності вразливості, список вразливих продуктів, тип загрози, що подається вразливістю, та іншу корисну інформацію). Порівняння дат публікації інформації про вразливість у базі даних NVD з інформаційними бюлетенями розробників вразливих програмних продуктів, у яких анонсується випуск виправлень для усунення вразливостей, показує, що ці дати переважно збігаються. Отже, було висунуто припущення про те, що дату публікації інформації про вразливість у базі NVD можна вважати датою випуску оновлення, що усуває вразливість. Водночас дату публікації інформації про вразливість у базі даних CVE (у форматі CVRF) можна вважати датою офіційного виявлення (розкриття) вразливості.

За основу під час об'єднання інформації про вразливість із різних джерел (CVE, CVRF і NVD), були прийняті такі допущення [12]: 1) датою розкриття вразливості вважати мінімальну з дат у розглянутих джерелах даних; 2) датою усунення вразливості вважати максимальну з дат урозглянутих джерелах даних. При цьому слід зазначити, що дати модифікації запису про вразливість не беруть участі в пошуку дат розкриття й усунення, оскільки вони не відображають стадію вразливості, а лише той факт, що цей запис було змінено.

Отримання дат виявлення і усунення вразливостей дає змогу застосувати апарат марковського моделювання та систем масового обслуговування для оцінювання рівня вразливості усієї комп'ютерної системи. У цілому алгоритм отримання цих параметрів на основі статистичного аналізу узагальненої бази даних про вразливості складається з таких етапів:

1) фільтрація вразливостей із досліджуваного програмного продукту й для необхідного інтервалу часу;

2) групування вразливостей за однією з дат, залежно від типу, від параметра, який потрібно отримати в результаті;

3) перерахунок абсолютної дати виявлення вразливості в інтервальну, відносно початку досліджуваного інтервалу, в годинах;

4) дослідження закону розподілу з оцінюванням значень його параметрів.

Для формування підмножин-вибірок вразливостей (на прикладі сімейства веб-серверів Apache) було застосовано такі критерії відбору:

– атрибут "cvss:access-vector" – значення мережне, (Network, N);

– атрибут "cvss:availability-impact" – значення часткове, (Partial, P) та повне, (Complete, C);

– атрибут "vuln:product" – значення "*Apache*";

– атрибут "vuln:published-datetime" – значення, що містить досліджуваний часовий проміжок (конкретний рік).

Для аналізу невеликої кількості вразливостей можна скористатися сторінкою розширеного пошуку в базі NVD [19]. У розширеному пошуку в базі дані видачі розділень на сторінки по 20 записів на кожній (рис. 3).

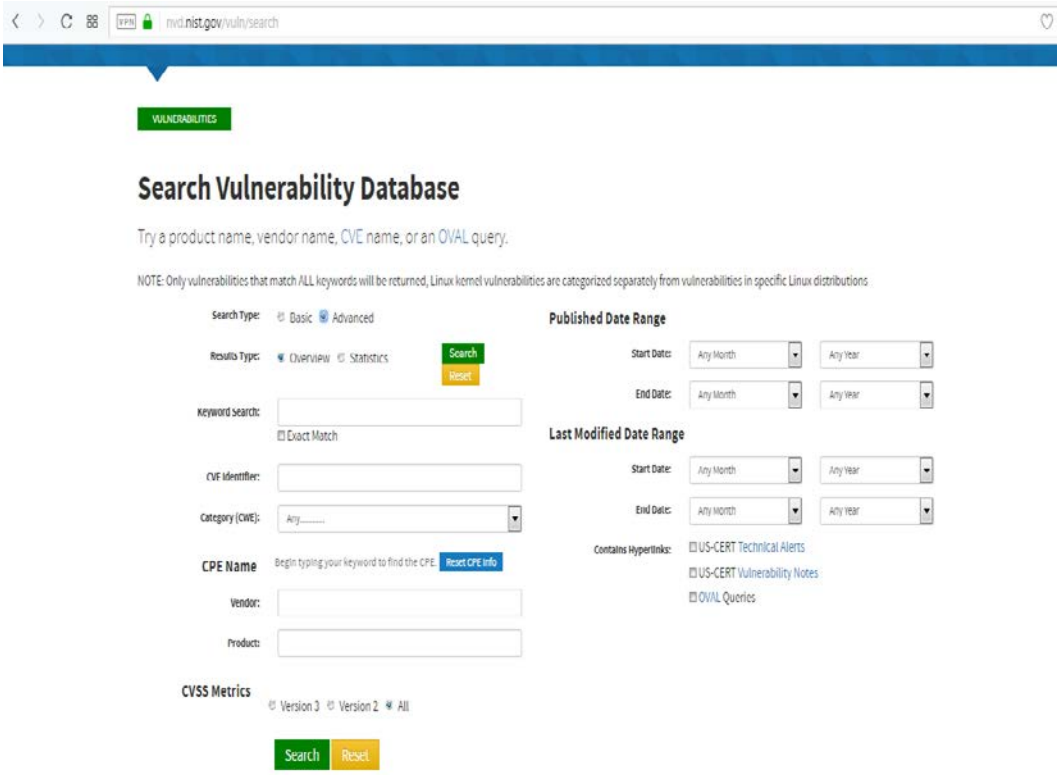

Рис. 3. Веб-інтерфейс розширеного пошуку NVD
для формування підмножин вразливостей доступності

Це суттєво ускладнює отримання й обробку вибірки великого обсягу та робить недоцільним ручну обробку даних для виконання поставлених завдань. Тому обрано більш прийнятний варіант обробки бази вразливостей у вигляді XML-документів. Для цього необхідно завантажити з сайту NVD архівний файл за відповідний рік. В отриманих у результаті фільтрації множинах вразливостей необхідно зафіксувати параметри “published” та “base_score”.

Було розглянуто дві вибірки з БД для вразливостей доступності сімейства веб-серверів Apache у 2015, 2016 рр. Результати оцінювання параметрів експоненціального розподілу отримано за допомогою інструментарію “Distribution fitting tool” пакета Matlab.

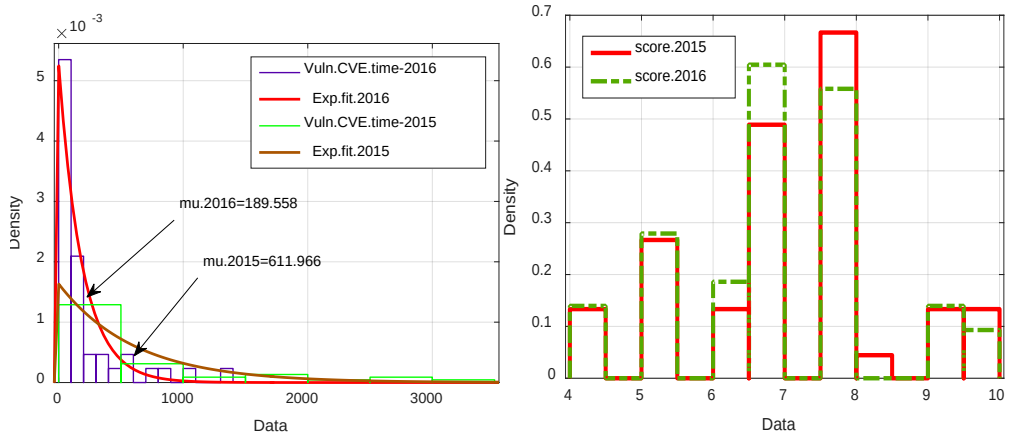

Рис. 4. Результати оцінювання параметрів вияву вразливостей доступності серверів Apachey 2015, 2016 рр.

Оскільки інформація про вразливості може надійти в базу як від спеціалістів з безпеки, так і після їх експлуатації зловмисниками, то час реєстрації вразливості відображає ступінь зацікавленості дослідниками конкретним елементом веб-сервера. Очевидна тенденція поступового зростання зацікавленості до мережених програмних продуктів, зокрема веб-серверів Apache [15]. Так, середній час реєстрації нових вразливостей доступності серверів Apachey 2016 р. скоротився у 3,23 раза порівняно з 2015 р. Також слід зазначити, що середня критичність вразливостей у 2015 р. (6,96) була більшою за цей же показник 2016 р. (6,78).

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Розглянуто питання параметризації вразливостей на основі вибірок із відкритих баз для використання у якості вхідних даних марковських моделей оцінювання доступності веб-ресурсів.

Проаналізовано актуальний стан зв'язків відкритої бази вразливостей CVE з іншими базами вразливостей. Визначено активність БД, їх відкритість, платний доступ чи можливість пробного/обмеженого використання. Розглянуто отримання та уточнення інформації з бази даних вразливостей NVD.

Виконано параметризацію вразливостей веб-серверів сімейства Apache на річних інтервалах 2015, 2016 рр. на основі вибірок із відкритих баз вразливостей. Результати дослідження показали, що у 2016 р. нові вразливості з вибірки фіксувалися у 3,23 раза швидше, але при цьому в середньому їхня критичність зменшилась на 3 %.

Для прискорення й зручнішою створення вибірок доцільно розробити програмне забезпечення, яке автоматично створюватиме необхідну вибірку після вибору критеріїв формування. Також для покращання результатів дослідження слід уточнювати інформацію про вразливість у декількох відкритих базах.

Список використаних джерел

1. *Присяжний Д. П.* Удосконалення захисту веб-ресурсів від атак на основі комбінованого евристично-статистичного підходу // Реєстрація, зберігання і обробка даних. 2016. Т. 18. № 1. С. 63–69.

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

3. Common Vulnerabilities and Exposures / The MITRE Corporation. URL: http://cve.mitre.org

4. Secunia Research Community / Flexera Software LLC. URL: https://secuniaresearch.flexerasoftware.com. 15.01.2019 p.

5. Security Focus database of computer security / SecurityFocus Symantec Corporate Offices. URL: http://www.securityfocus.com

6. Exploit Database by Offensive Security / Exploit Database by Offensive Security. URL: https://www.exploit-db.com

7. Microsoft Security Bulletins / Microsoft Corporation. URL: https://docs.microsoft.com/en-us/ security-updates/securitybulletins/securitybulletins

8. CERT Vulnerability Notes Database / Carnegie Mellon University Software Engineering Institute. URL: https://www.kb.cert.org/vuls

9. Android Security Bulletins / Android by Google LLC and the Open Handset Alliance. URL: https://source.android.com/security/bulletin

10. National vulnerability database / NIST Computer Security Division, Information Technology Laboratory. URL: https://nvd.nist.gov

11. *Федорченко А. В., Чечулин А. А., Котенко И. В.* Построение интегрированной базы уязвимостей // Известия вузов. Приборостроение. 2014. Т. 57. № 11. С. 62–67.

12. *Белобородов А. Ю., Горбенко А. В.* Применение баз данных уязвимостей в задачах исследования безопасности программных средств // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. 2015. Вип. 165. С. 83–85.

13. *Алаа Мохаммед Абдул-Хади, Поночовный Ю. Л., Харченко В. С.* Разработка базовых марковских моделей для исследования готовности коммерческих веб-сервисов // Радіоелектронні і комп'ютерні системи. 2013. Вип. 5 (64). С. 186–191.

14. *Царегородцев А. В., Макаренко Е. В.* Методика количественной оценки риска в информационной безопасности облачной инфраструктуры организации // Дайджест-финансы. 2015. № 1 (233). С. 56–67.

15. *Kharchenko V., Ponochovnyi Y., Mustafa Qahtan Abdulmunem A.-S., Andrashov A.* Availability models and maintenance strategies for smart building automation systems considering attacks on component vulnerabilities // Advances in Intelligent Systems and Computing. 2018. Vol. 582. P. 186–195.

16. *Алаа Мохаммед Абдул-Хади.* Оценка интенсивности атаки на уязвимости доступности коммерческих веб-сервисов // Системи обробки інформації. 2013. Вип. 6 (113). С. 204–208.

17. *Харченко В. С., Алаа Мохаммед Абдул-Хади, Поночовный Ю. Л.* Формирование подмножеств уязвимостей доступности коммерческих веб-сервисов // Системи обробки інформації. 2013. Вип. 8 (115). С. 240–243.

18. CVE Reference Key/Maps / The MITRE Corporation. URL: https://cve.mitre.org/data/refs/index.html

19. NVD – Search and Statistics / NIST Computer Security Division, Information Technology Laboratory. URL: https://nvd.nist.gov/ vuln/search

References:

1. Prisyashniy D. P. (2016), *"Udoskonalennya zakhystu veb-resursiv vid atak na osnovi kombinovanoho evrystychno-statystychnoho pidkhodu"* ["Improving the protection of web resources from attacks on the basis of a combined heuristic-statistical approach"], Collection of scientific works *Reyestratsiya, zberihannya i obrobka danykh* [Registration, storage and processing of data], tom 18, vol. 1, pp. 63–69 [Ukraine].

2. Fedorchenko A. V., Chechulin A. A. and Kotenko I. V. (2014.), *"Issledovaniye otkrytykh baz uyazvimostey i otsenka vozmozhnosti ikh primeneniya v sistemakh analizazashchishchennosti komp'yuternykh setey"* ["Study of open databases of vulnerabilities and assessment of their applicability in computer security analysis systems"], Journal *Informatsionno-upravlyayushchiye sistemy* [Information Control Systems], vol. 5, pp. 72–79 [Russia].

3. Common Vulnerabilities and Exposures / The MITRE Corporation, available at: http://cve.mitre.org – 15.01.2019.

4. Secunia Research Community / Flexera Software LLC, available at: https://secuniaresearch.flexerasoftware.com – 15.01.2019.

5. SecurityFocus database of computer security / SecurityFocus Symantec Corporate Offices, available at: http://www.securityfocus.com – 15.01.2019.

6. Exploit Database by Offensive Security / Exploit Database by Offensive Security, available at: https://www.exploit-db.com - 15.01.2019.

7. Microsoft Security Bulletins / Microsoft, available at: https://docs.microsoft.com/en-us/security-updates/securitybulletins – 15.01.2019.

8. CERT Vulnerability Notes Database / Carnegie Mellon University Software Engineering Institute, available at: Access mode: https://www.kb.cert.org/ vuls – 15.01.2019.

9. Android Security Bulletins / Android by Google LLC and the Open Handset Alliance, available at: https://source.android.com/security/bulletin – 15.01.2019.

10. National vulnerability database / NIST Computer Security Division, Information Technology Laboratory, available at: https://nvd.nist.gov – 15.01.2019.

11. Fedorchenko A. V., Chechulin A. A. and Kotenko I. V. (2014), *"Postroyeniye integrirovannoy bazy uyazvimostey"* ["Building Integrated Vulnerability Base"] Collection of scientific works *Izvestiya vuzov. Priborostroyeniye* [Izvestiya Vuzov. Instrument making], vol. 57, No. 11, pp. 62-67 [Russia].

12. Beloborodov A. Yu. and Gorbenko A. V. (2015), *"Prymenenye baz dannykh uyazvymostey v zadachakh yssledovanyya bezopasnosty prohrammnykh sredstv"* ["Using vulnerability databases in software security research tasks"], *Visnyk Kharkivs'koho natsional'noho tekhnichnoho universytetu sil's'koho hospodarstva imeni Petra Vasylenka* [Bulletin of Kharkiv National Technical University of Peter Vasilenko], vol. 165, pp. 83–85 [Ukraine].

13. Alaa Mohammed Abdul-Hadi, Ponochovny Yu. L. and Kharchenko V. S. (2013), *"Razrabotka bazovykh markovskikh modeley dlya issledovaniya gotovnosti kommercheskikh veb-servisov"* ["Development of basic Markov models for the study of the availability of commercial web services"], Journal *Radíoyelektronní í komp'yuterní sistemi* [Radio and Computer and Computer Systems, vol. 5 (64), pp. 186–191 [Ukraine].

14. Tsaregorodtsev A. V. and Makarenko E. V. (2015), *"Metodika kolichestvennoy otsenki riska v informatsionnoy bezopasnosti oblachnoy infrastruktury organizatsii"* ["Method of quantitative risk assessment in the information security of the organization's cloud infrastructure"], Journal *Daydzhest-finansy* [Digest Finance], vol. 1 (233), pp. 56–67 [Russia].

15. Kharchenko V., Ponochovnyi Yu., Mustafa Qahtan Abdulmunem A.-S. and Andrashov A. (2018), "Availability models and maintenance strategies for smart building automation systems considering attacks on component vulnerabilities", Advances in Intelligent Systems and Computing, vol. 582, pp. 186–195.

16. Alaa Mohammed Abdul-Hadi (2013), *"Otsenka intensivnosti ataka na uyazvimosti dostupnosti kommercheskikh veb-servisov"* ["Assessment of the intensity of the attack on the vulnerability of the availability of commercial web services"], Journal *Systemy obrobky ínformatsíi* [Processing Systems Information], vol. 6 (113), pp.204–208 [Ukraine].

17. Kharchenko V. S. Alaa Mohammed Abdul-Hadi and Ponochovny Yu. L. (2013), *Formirovaniye podmnozhestv uyazvimostey dostupnosti kommercheskikh veb-servisov* ["Formation of subsets of accessibility vulnerabilities in commercial web services"], Journal *Sistemi obrobki ínformatsíí*