УДК 004.056
DOI: 10.31673/2409-7292.2019.024246

Л.А. Асєєва

АНАЛІЗ ОСНОВНИХ СКЛАДОВИХ НЕБЕЗПЕКИ ПРИ ПОБУДОВІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В роботі проведено аналіз основних складових небезпеки в системі інформаційної безпеки підприємств, до яких віднесено атаки, загрози та вразливості. На основі сучасного стану досліджень розглянуті поширені списки та класифікатори атак і вразливостей, які дозволяють фаховій спільноті використовувати їх для опису та дослідження складових небезпеки. Результати роботи можуть бути застосовані для аналізу існуючих загроз та опису складових системи управління інформаційної безпеки окремого підприємства.

Ключові слова: інформаційна безпека, класифікація, загроза, атака, вразливість.

Вступ

Прийняття запобіжних заходів щодо реалізації так званої тріади цілей інформаційної безпеки, що полягає в забезпеченні конфіденційності, цілісності, доступності інформації є основним підходом у створенні систем кібербезпеки. З використанням персональних комп'ютерів та Інтернету виникли та продовжують вдосконалюватися нові прийоми добре обізнаних у відповідній області та високо мотивованих суб'єктів незаконного отримання інформації [1]. Якщо раніше для цього необхідно було заволодіти і винести з об'єкта цілі купи паперових документів, або їх копій, подолати розвинуті перепони системи контролю фізичного доступу до місця знаходження інформації, то зараз величезні обсяги важливих відомостей можна просто «злити» на флешку, що міститься в брелоку, відправити по мережі, вдавшись до використання сімейства руткітів, троянів, бекдор, кейлоггеров і ботнетів, отримати віртуальний доступ, або їх знищити за допомогою вірусів, влаштувавши атаку. Оскільки інформація у системі цінностей людства загалом та кожної людини окремо вже посідає одну з найвищих позицій, ії захист потребує уваги і постійного розвитку. Щоб створювати та вдосконалювати ефективні системи інформаційної безпеки підприємств необхідно проаналізувати основні складові небезпеки.

Основна частина

Метою даної роботи є аналіз основних складових небезпеки при побудові системи інформаційної безпеки підприємства. Для досягнення поставленої мети в роботі розглянуті деякі різновиди атак, вразливостей та загроз, що є основними складовими кібербезпеки, наведені та описані поширені списки та класифікатори, що дозволяють фаховій спільноті використовувати їх для опису та дослідження складових небезпеки.

Ключові складові небезпеки

Центром уваги фахівців у галузі кібербезпеки визначено атаки, загрози, та вразливості.

Під атакою більшість авторів розуміють навмисне використання виявлених вразливостей чи спробу реалізації існуючих загроз комп'ютерних інформаційних систем як з конкретною метою, так і просто для розваги.

За визначення CERT загрозами є будь-які обставини або події, які можуть спричинити шкоду системі або мережі.

Вразливості визначаються як [1]:

а) функція або помилка в системі або програмі, яка дозволяє зловмисникам обходити заходи безпеки;

б) аспект системи або мережі, що залишає її відкритою для атаки;

в) відсутність або слабкість ризику зменшення гарантій, які мали б потенціал для того, щоб загроза могла відбуватися з більшою частотою чи більшим впливом;

д) вада, яка робить ціль атаки сприйнятливою до нападу.

Три зазначені складові в кіберпросторі атаки, загрози, та вразливості є ключовими сутностями в структурі небезпеки та одночасно явищами через які небезпека реалізується.

У кіберзлочинців можуть бути різні мотиви для вибору цілі атаки. Вони постійно шукають та виявляють вразливі системи. Існуючі міжнародні кримінальні мережі спричиняють збитки, що обчислюються в мільярдах доларів [2] [3].

Незалежно від того, чи буде об'єкт атаки великою корпорацією або мікро-бізнесом, жодна організація не може бути гарантовано уникнути перевірки хакерів[4].

Класифікатори та рейтинги вразливостей

Слабкі сторони програмного забезпечення – це помилки, які можуть призвести до вразливості програмного забезпечення. Вразливості програмного забезпечення, що перераховані в списку Common Vulnerabilities and Exposures (CVE), є помилками в програмному забезпеченні, які можуть бути використані зловмисником для доступу до системи або мережі [5]. Цей список є розробкою The MITRE Corporation, що спеціалізується в області системної інженерії та веде розробки й дослідження в інтересах органів державної влади США, таких як Міністерство оборони США, Федеральне управління цивільної авіації США та на замовлення Міністерства внутрішньої безпеки США і розвивається при широкій підтримці спільноти експертів. В результаті роботи сканерів вразливостей різних розробників перелік знайдених помилок описується із використанням списку CVE, чим дозволяє порозумітися фахівцям при описуванні явищ та допомагає уникати неоднозначності.

Результатом продовження роботи MITRE над CVE стала розробка CWE .

Призначений для розробників і фахівців щодо забезпечення безпеки програмного забезпечення загальний перелік вразливостей і недоліків безпеки програмного забезпечення створено й поширено в фаховому середовищі CWE (Common Weakness Enumeration) у вигляді ієрархічного словника [6]. В оновленні переліку бере участь велика кількість компаній-постачальників операційних систем, постачальників інструментів комерційної інформації, наукових кіл, урядових установ і дослідницьких установ. Оновлення відбувається через поштову розсилку за допомогою широкого обговорення на офіційному форумі CWE. За визначенням розробників, CWE - це спільна мова для опису недоліків безпеки програмного забезпечення, яка необхідна для стандартизації методик оцінки програмних продуктів, що важливо не тільки веб-додатків, а й інформаційних систем взагалі. Відомі вендори Symantec, Apple, HP і EMC публічно заявили, що використовують CWE у своєму життєвому циклі розробки програмного забезпечення (SDLC), чим визначили та підкреслили актуальність проблеми систематизації недоліків та вразливостей. Ідентифікатори CWE використовуються ними для відстеження проблем, що виникають під час діяльності з розробки програмних продуктів.

Важливою особливістю CWE є сувора структурованість. Будь-яка зміна є результатом об'ємної роботи спільноти, тому перелік оновлюється відносно рідко.

Для класифікації недоліків використовується багаторівнева структура, яка описує деревоподібний вид CWE: кінцеві недоліки об'єднуються в варіанти, варіанти - в категорії, категорії - в представлення. Кожне представлення - особливий спосіб класифікації записів CWE, призначений для спрощення вирішення конкретного завдання. В останній версії три основних подання представлення концепцій: розробки, архітектури та досліджень.

В межах представлення концепції розробки недоліки безпеки в CWE класифікуються з використанням принципів і понять, які часто зустрічаються при розробці програмного забезпечення, що корисно в першу чергу для розробників і фахівців з оцінки якості програмного забезпечення.

Представлення концепції архітектури використовується для аналізу якості архітектурних рішень на етапі проектування.

Представлення концепції досліджень сформовано для спрощення академічних досліджень. Відрізняється від перших двох високим рівнем абстракцій. Основна увага в цьому поданні приділена формальним поняттям поведінки програмного забезпечення, конкретні ж приклади часто опускаються. На рис.1 нижче наведено як приклад граф зв'язків

CWE-611 (XXE Неправильне обмеження у посиланні на зовнішні об'єкти XML) в різних представленнях.

Оскільки CWE претендує на те, щоб бути найбільш загальним переліком недоліків безпеки, велика увага при розробці класифікатора звертається на зіставлення записів CWE із записами інших класифікацій, переліків, каталогів. Результатом цього зіставлення є представлення зовнішніх відображень, наприклад, SANS Top 25, OWASP Top 10, Seven Pernicious Kingdoms та ін [7]. Ці представлення переносять структуру інших рейтингів і класифікацій на CWE для того, щоб спростити їх порівняння і роботу з ними. Розширення та збагачення CWE відбувається через обговорення на офіційному форумі і через цілеспрямовані поштові розсилки авторизованим учасникам.

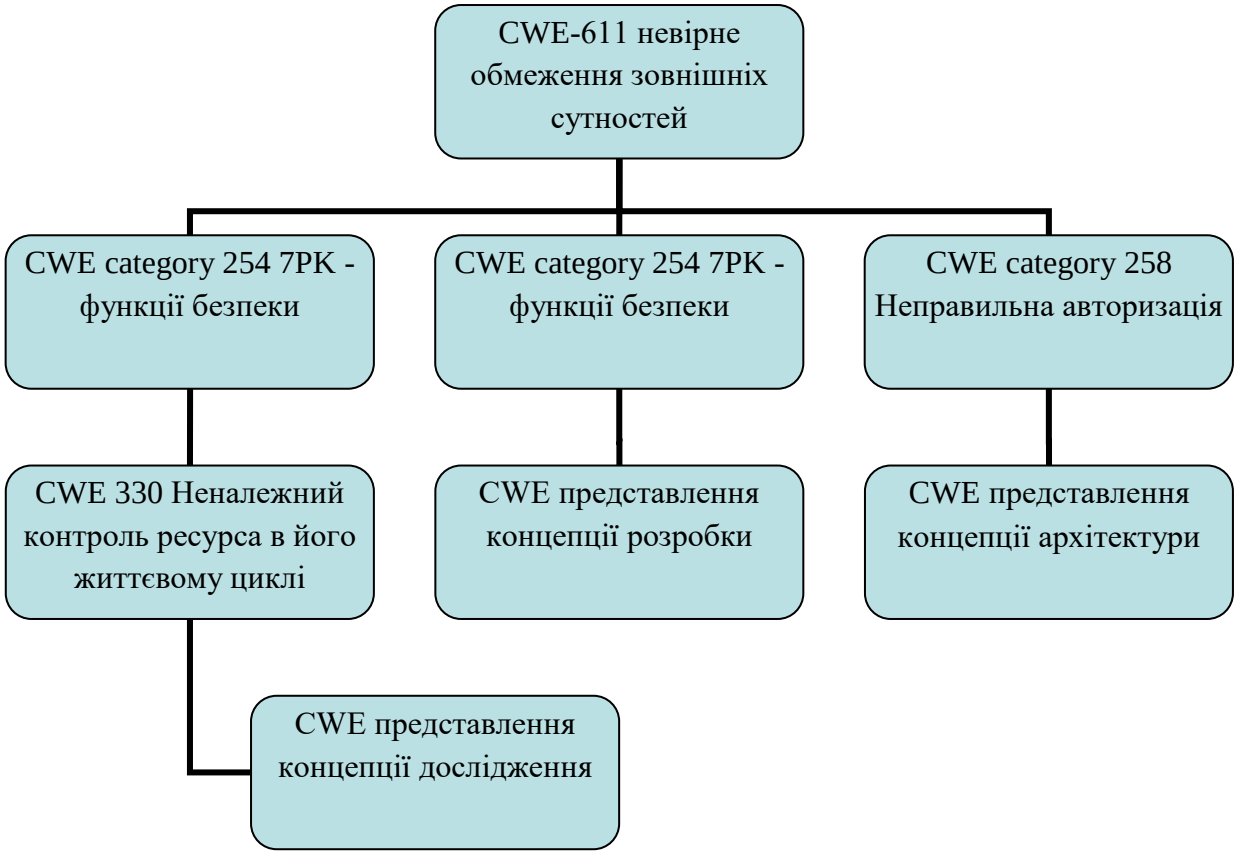

Рис. 1. Граф зв'язків CWE-611

CWE використовується багатьма інструментами статистичного аналізу, оцінки якості та безпеки програм, більшість з таких інструментів зареєстрована в MITRE як CWE-сумісні. CWE служить спільною мовою розробників, практиків безпеки, аналітиків та викладачів для опису слабкості безпеки програмного забезпечення в архітектурі, дизайні або коді; служить в якості стандартної мірної палички для програмних засобів безпеки, орієнтованих на ці недоліки; забезпечує використання спільного базового стандарту для виявлення слабкостей, послаблення та профілактики впливів.

Приклад побудованого графу CWE -254 для вразливості відомого протоколу WPA2 [8] відповідно до позицій списку CVE 2017-13077- CVE 2017-13088 представлено на рисунку 2.

В основному зловмисники намагаються отримати контроль над веб-додатком, обліковим записом або хостом в цілому та підготуватись до наступних етапів атак. В 2018 році OWASP зосередило увагу на питаннях безпеки, які виникли внаслідок швидкого, широкого поширення нових технологій, таких як API, контейнери та хмарні сервіси. Це

також впливає на розвиток векторів атаки та автоматизованих процесів розробки програмного забезпечення.

Спеціалісти з кібербезпеки постійно обмінюються досягненнями та вдосконалюють опис вразливостей, які виявили за допомогою комплексів відкритих платформ. Цінність однієї із них Bugcrowd [9] визначено в ефективному використанні креативності глобального натовпу хакерів - спільноти, що названі як білі капелюхи, за свої цілі й прагнення у покращені безпеки, та завзятості перехитрити противників. Результати, що отримані з Bugcrowd, не можна отримати за допомогою традиційного тестування безпеки, вони систематизуються й публікується в рейтингу VRT Bugcrowd, таким чином фахівцям у всьому світі повідомляється про серйозність виявлених проблем безпеки.

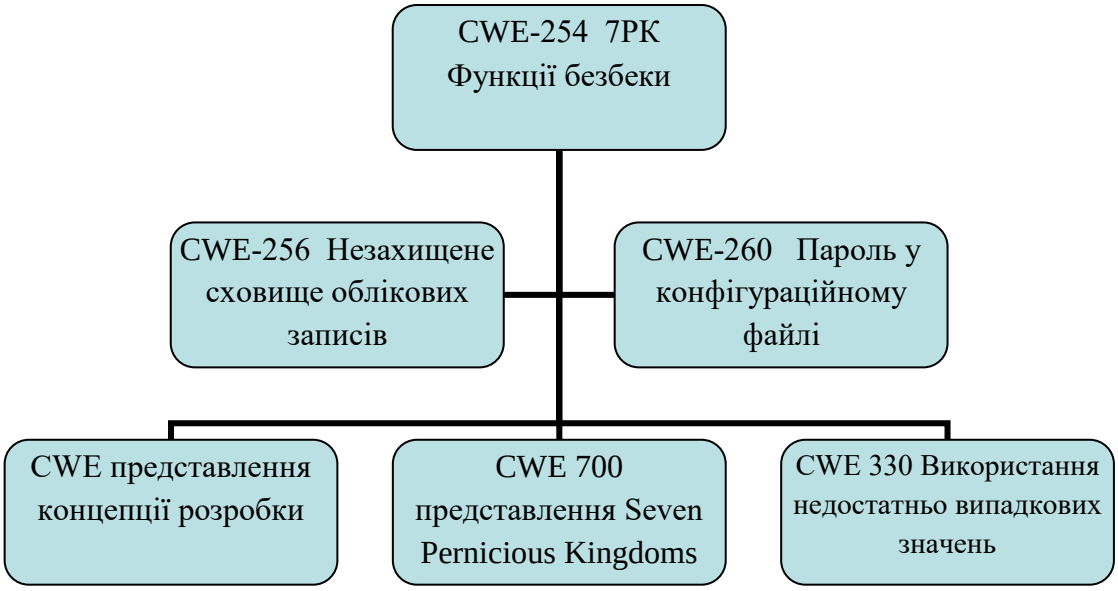

Рис. 2. Граф зв'язків CWE-254

Важливо, що опис вразливостей за рейтингом VRT Bugcrowd показано у відповідності до попередньо переліку за OWASP та майже одночасно оновленим із рейтингом у 2018 році класифікатора CWE.

Класифікатор атак

Важливим для ефективної кібербезпеки є розуміння того, як діє противник, тому цей класифікатор є систематизацію шаблонів атак, тобто опису загальних елементів і методів, що використовуються при атаках на вразливі компоненти. В ході вдосконалення CWE з'явилася ще одна класифікація, схожа з CWE за структурою - CAPEC (Common Attack Pattern Enumeration and Classification). Вона може бути використана аналітиками, розробниками, тестерами та педагогами для просування накопичених знань спільноти та підвищення захисту. Розширення переліку відбувається аналогічно CWE через обговорення на офіційному форумі та поштову розсилку.

У CAPEC використовується схожий з CWE ієрархічний підхід. Розроблено два основних представлення (механізми атак і об'єкти атак) та кілька допоміжних. У представленні механізмів атак шаблони ієрархічно впорядковані відповідно до механізмів, які часто використовуються при експлуатації вразливостей. Категорії, наприклад «впровадження непередбачених елементів», в цьому представленні відображають різні методи, що використовуються для атаки на систему, але не відображають цілей і наслідків. У представленні об'єктів атак категорії містять опис компонентів, на які проводиться атака, наприклад «передача даних».

Опис кожного шаблону містить наступні елементи: короткий опис можливих дій зловмисника, тип важкості, перелік відносин зі схожими шаблонами, передумови, що визначають можливість атаки, відповідність ресурсів, на які спирається механізм атаки, посилання на відповідні вразливості у CWE.

Враховуючи зацікавленість фахівців з інформаційної безпеки у виявленні джерела та організаторів атак для подальшого притягнення до відповідальності на підставі юридично допустимих доказів, створення та вдосконалення вищеописаних класифікаторів й списків дозволяють фахівцям формувати перспективні напрямки розвитку кібербезпеки та кіберпростору в цілому. Класифікатори CWE та CAPEC в першу чергу призначені для аналізу та оцінки програмного забезпечення, яке є ще тільки в процесі розробки, у порівнянні з фокусуванням списку CVE на програмних помилках вже запущених комерційних і загальнодоступних відкритих проектів.

Висновки

Таким чином, в роботі розглянуті поширені списки та класифікатори вразливостей і атак, які можуть бути використані для опису та дослідження складових небезпеки.

Результати роботи можуть бути покладені в основу аналізу існуючих загроз інформаційної безпеки та опису складових системи управління інформаційної безпеки окремого підприємства та розробки комплексу заходів для їх попередження.

Список використаної літератури

1. Cherian Samuel. “Cybersecurity: Global, Regional and Domestic Dynamics “.Institut for Defence Studies and Analyses. New Delhi. Monograph series No42.dec2014.pp10 84c.
2. Kevin Granville “Recent cyberattacks”. feb. 5,2015 URL: https://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html?_r=1
3. Ben Rossi “Top 10 most devastating cyber hacks of 2015”. Dec. 10,2015 URL: https://www.information-age.com/top-10-most-devastating-cyber-hacks-2015-123460657/
4. James A. Lewis “Rethinking Cybersecurity: Stratedy, Mass Effect and States”.CSIS. Jan. 2018. 50c.
5. Cve details. URL: https://www.cvedetails.com/vulnerability-search.php
6. CWE List .View the List of Weaknesses URL: https://cwe.mitre.org/data/index.html Apr. 13 2018.
7. Топ-10 OWASP URL: https://www.imperva.com/app-security/owasp-top-10/
8. Mathy Vanhoef. “Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse. imec-DistriNet.” KU Leuven. 2017 . URL : https://www.krackattacks.com/
9. Bugcrowd Vulnerability Rating Taxonomy by Bugcrowd.com v1.4. Apr. 13 2018. URL: https://bugcrowd.com/vulnerability-rating-taxonomy.

Надійшла: 03.06.2019 Рецензент: д.т.н., доц. Гайдур Г.І.