УДК 621.391: 004.056.5

АНАЛІЗ МЕТОДІВ КЛАСИФІКАЦІЇ ВРАЗЛИВОСТЕЙ ТА ЗАГРОЗ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Румянцева Ольга Володимирівна
студентка VI курсу факультету Інфокомунікацій
Харківський національний університет радіоелектроніки, Україна
Пшеничних Сергій Васильович
кандидат технічних наук, старший науковий співробітник, доцент кафедри інфокомунікаційної інженерії
імені В.В. Поповського
Харківський національний університет радіоелектроніки, Україна

Анотація. У тезах розглядаються відомі методи класифікації вразливостей та загроз інформаційної системи, які можна використовувати для нейтралізації виявлених уразливостей за рахунок налаштування засобів захисту, резервування, розробки організаційних заходів. Також класифікація дозволяє чітко визначити, чому саме має протистояти система захисту інформації.

Ключові слова: інформаційні технології, інформаційна система, система захисту інформації, вразливість, загроза.

У сучасних умовах розвитку інформаційних технологій при створенні інформаційних систем (ІС) для комерційних чи державних організацій обов'язково створюється система захисту інформації (СЗІ). На етапі проектування ІС виникає питання ефективності СЗІ, створеної за тим чи іншим проектом. Вирішення завдання формального порівняння кількох проектів СЗІ для вибору найкращого викликає певні складнощі.

Крім того, існує безліч сучасних міжнародних та вітчизняних стандартів та нормативних документів у галузі інформаційної безпеки, що розглядають питання оцінки ефективності СЗІ або визначають вимоги до її функціональності. У цих документах, як правило, як критерій ефективності використовується наявність тих чи інших засобів захисту інформації або вимоги до їх параметрів і не враховується, що є можливості подолання даних засобів за рахунок наявності в них та ІС тих чи інших вразливостей. Таким чином, актуальним є завдання вибору оптимального проекту СЗІ за критерієм ефективності, що враховує наявність вразливостей та взаємозв'язків між ними.

Процес функціонування типової організації полягає у постійній обробці великих обсягів інформації, їх аналізі, прийнятті рішень та управлінської діяльності. Для автоматизації процесів функціонування типової організації створюється ІС.

Під ІС розуміється організаційно впорядкована сукупність документів (масивів документів) та інформаційних технологій, у тому числі з використанням засобів обчислювальної техніки та зв'язку, що реалізують процеси збирання, накопичення, обробки, пошуку та розповсюдження інформації [1].

Процес реалізації загрози ІС пов'язаний з послідовним використанням вразливостей. Вразливості існують у різних структурних елементах ІС та програмної або апаратної складової елементів ІС.

Для дослідження процесів безпеки інформації досліджується структура ІС, її складові та їх взаємодія. ІС різняться залежно від масштабів, способу організації чи сфери діяльності. Відповідно, для побудови моделей, що відображають особливості структури та функціонування досліджуваної ІС необхідно визначити до якого класу належить типова ІС організації.

Основу ІС складають територіально розподілені комп'ютерні системи (обчислювальні мережі) елементи яких розташовані в окремих будівлях, на різних поверхах цих будівель і пов'язані між собою транспортним середовищем, яке використовує фізичні принципи («вита пара», оптико-волоконні канали, радіоканал і т.д.). Основу апаратних (технічних) засобів таких систем складають електронно-обчислювальні машини (ЕОМ) або групи ЕОМ, периферійні, допоміжні пристрої та засоби зв'язку, що сполучаються з ЕОМ.

У процесі функціонування ІС часто виникають загрози безпеці інформації. Під загрозою безпеці інформації, при цьому, розуміється подія або дія, яка може спричинити зміну функціонування ІС, пов'язану з порушенням захищеності інформації, що обробляється [2]. Джерелами виникнення загроз можуть бути форс-мажорні обставини, збої у роботі обладнання, помилки персоналу та, безумовно, навмисні дії зловмисників.

Для запобігання реалізації загроз створюються комплексні системи захисту інформації (КСЗІ). Під КСЗІ розуміється комплекс організаційних, інженерно-технічних, технічних і програмних заходів спрямованих на підтримку захищеності інформації [3].

КСЗІ інформаційних систем створюються згідно з директивно заданою для цієї організації концепцією захисту інформації. Концепція задає регламент використання комплексу взаємообґрунтованих та узгоджених нормативно-організаційних і технічних заходів щодо запобігання витоку інформації при її обробці, зберіганні та передачі [4].

При розробці проектів систем захисту інформації важливим завданням є визначення вразливостей існуючої інформаційної системи та передбачуваних до застосування засобів та методів захисту. Це необхідно для нейтралізації виявлених вразливостей за рахунок, наприклад, налаштування засобів захисту, резервування, розробки організаційних заходів та інш. Для більш повного аналізу виявлених вразливостей проводиться їх класифікація. При цьому існує безліч підходів до класифікації вразливостей, в яких використовується безліч класифікаційних параметрів, таких як:

— етап життєвого циклу інформаційної системи, у якому впроваджується вразливість;

— рівень в інфраструктурі інформаційної системи;

— рівень небезпеки вразливості;

— причина виникнення;

— особливості вразливості;

— місцезнаходження.

Аналіз наведених підходів до класифікації показує наступне:

— класифікація за етапом життєвого циклу, на якому виникає вразливість, зачіпає всі можливі вразливості ІС. Однак її практичне застосування може бути скрутним, тому що вона є надмірно узагальненою. Відповідно, класи, що виходять, будуть занадто великими;

— класифікація за рівнем в інфраструктури ІС зосереджується на програмних та програмно-апаратних засобах захисту та ігнорує організаційні та технічні засоби захисту та їх вразливості;

— класифікація за рівнем небезпеки зосереджується виключно на вразливості програмного забезпечення, залишаючи поза розгляду вразливості інших складових системи захисту інформаційної системи;

— різні підходи до класифікації через виникнення об'єднує те, що всі вони зосереджені на описі вразливостей операційних систем та програмного забезпечення і, відповідно, не розглядають вразливості організаційних, технічних та апаратних засобів та методів захисту інформації.

— класифікація організації, MITRE за різними особливостями властивих вразливостей (список CWE) також стосується лише вразливості програмного забезпечення [5];

— класифікації за місцезнаходженням поділяють вразливості щодо того, в якій частині ресурсів інформаційної системи вони знаходяться (програмної чи апаратної), відповідно до класифікації не зачіпають вразливостей пов'язаних з помилками в організації захисту інформації.

Основним критерієм порівняння для класифікації вразливостей, з практичної точки зору, є максимальне охоплення класифікацією вразливостей ІС.

Таким чином, класифікація тільки за однією класифікаційною ознакою призводить або до того, що розглядається лише частина вразливостей інформаційної системи, або до того, що вразливості розбиваються на надмірно великі класи, елементи яких (тобто вразливості) можуть сильно відрізнятися один від одного.

Отже, переважно використовувати такі класифікації, які розглядали одночасно кілька класифікаційних ознак. До таких класифікацій належать: класифікація вразливостей Landwehr'a [6] та узагальнена класифікація вразливостей [7]. Перевагою узагальненої класифікації є те, що вона розглядає і вразливості організаційного захисту, хоча й не наводить їх докладнішої класифікації. Таким чином, узагальнена класифікація вразливостей охоплює практично всі аспекти проблеми вразливостей ІС. У свою чергу, недостатня подробиця того чи іншого підкласу може бути вирішена його розширенням. Відповідно, дана класифікація найбільше підходить для практичного застосування.

Також важливим завданням при розробці систем захисту є визначення загроз для інформаційної системи, що захищається, що дозволяє чітко визначити чому саме повинна протистояти система захисту. Як наслідок, також необхідно проводити класифікацію загроз.

Аналіз літератури показує, що є безліч підходів до класифікації загроз. При цьому в цих підходах до класифікації простежується неоднозначність визначення загрози безпеці інформації. Існує два визначення загрози безпеці інформації. Під загрозою безпеки інформації розуміється сукупність умов та факторів, що створюють потенційну або реально існуючу небезпеку, пов'язану з витоком інформації, та/або з несанкціонованим та/або ненавмисним впливом на неї [8]. Та під загрозою безпеки інформації розуміється подія чи дія, що може викликати зміну функціонування ІС пов'язані з порушенням захищеності оброблюваної у ній інформації, тобто. з негативним впливом неї. Під негативною дією розуміється порушення фізичної цілісності, логічної структури, несанкціоноване отримання, модифікація тощо [9].

Аналіз даних визначень показує, що у першому визначенні розглядається деяка сукупність чинників, тобто. фактично поняття загрози інформації поєднується з поняттям вразливостей системи захисту, типом зловмисника, його оснащенням та здібностями, системою захисту та її налаштуваннями тощо. Спільно ці чинники призводять до існування небезпек.

У другому визначенні під загрозою розуміється деяка подія, що виникає в системі і веде до деяких негативних наслідків.

Таким чином, визначення загрози інформаційної безпеки, що використовується, впливає на вибір класифікаційних ознак.

У разі, коли під загрозою розуміється сукупність факторів, що призводять до завдання шкоди інформації, як класифікаційна ознака використовується будь-який з подібних факторів, або їх сукупність. При цьому виділяються такі ознаки, як:

— джерела загроз;

— кошти, що застосовуються для реалізації загроз;

— способи, що застосовуються для реалізації загроз;

— етапи життєвого циклу, на яких відбувається реалізація загрози;

— випадковість.

У разі, коли під загрозою розуміється подія, яка веде до завдання шкоди інформації. Як класифікаційна ознака виділяються:

— вид завданих збитків (результат реалізації загрози);

— спрямованість загроз.

Також є підходи до класифікації загроз, у яких використовується відразу кілька класифікаційних параметрів. До них відносяться класифікація загроз для розподілених обчислювальних систем та системна класифікація загроз [10,11].

Враховуючи концепцію здійснення загрози, в якій поняття загрози відокремлено від поняття вразливості, основним критерієм для порівняння є визначення загрози інформаційній безпеці, що лежить в основі класифікації. Виходячи з прийнятого критерію порівняння, вибираються підходи щодо виду збитків, спрямованості загроз, загроз для розподілених обчислювальних систем і системна класифікація загроз.

На жаль, всі виявлені підходи не розглядають взаємозв'язок між загрозами, тобто. в них не знаходить відображення той факт, що реалізація загрози може призвести до реалізації інших загроз. Наприклад, загроза розкрадання жорсткого диска з даними призводить одночасно до реалізації загроз розкриття конфіденційності даних, що зберігаються на диску. У наведених класифікаціях дані загрози будуть у різних класах і поміж них не буде встановлено явного зв'язку.

Таким чином, виникає необхідність у розробці такої моделі чи класифікації загроз, яка у явному вигляді визначала б взаємозв'язки між різними загрозами.

Список джерел:

1. Грищук, Р. В. Основи кібербезпеки / Р. В. Грищук, Ю. Г. Даник // – Ж.: ЖНАЕУ, 2016. – 688 с.
2. Молодецька, К. В. Соціальні інтернет-сервіси як суб’єкт інформаційної безпеки держави / К. В. Молодецька // Information technology and security. – 2016. – Vol. 4, Iss. 1. – С. 13–20.
3. Молодецька, К. В. Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах / К. В. Молодецька // Проблеми інформаційних технологій. – 2016. – № 20. – С. 84– 93.
4. Молодецька-Гринчук, К. В. Виявлення інформаційних впливів у соціальних інтернет-сервісах на основі інтелектуального аналізу текстового контенту / К. В. Молодецька-Гринчук // Актуальні питання забезпечення кібербезпеки та захисту інформації. – 2017. – С. 121–122.
5. Молодецька-Гринчук, К. В. Методика виявлення маніпуляцій суспільною думкою у соціальних інтернет-сервісах / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2016. – № 24. – С. 80–92.
6. Молодецька-Гринчук, К. В. Метод побудови профілів інформаційної безпеки акторів соціальних інтернет-сервісів / К. В. Молодецька-Гринчук // Інформаційна безпека. – 2017. – № 26. – С. 104–110.
7. . Hells U., Karras A., Scherer K.R. Multichannel communication of emotion: synthetic signal production // Facets of Emotion. Recent research / Ed. K.R.Scherer/ — Hillsdate, N.J. — 1988. — P. 162.
8. Council of Europe Convention on Access to Official Documents, Tromso, 2009 / / CETS № 205.
9. Cooruption, Inequality, and the Rule of Law : The Building Pocket Makes the Easy Life / By Eric M. Uslaner. — Cambridge University Press, 2008. — 360 p.].
10. Cooruption, Inequality, and the Rule of Law : The Building Pocket Makes the Easy Life / By Eric M. Uslaner. — Cambridge University Press, 2008. — 390 p.].

11. Breslin, Brigid ; Doron Ezickson ; John Kocoras (2010). «The Bribery Act 2010 raising the bar above the US Foreign Corrupt Practices Act». Company Laweyr. Sweet & Maxwell. 31 (II) . ISSN 0144-1027 C. 35.].