УДК: 340.13
І.Л. Обертинюк, О.В. Кареліна канд. пед. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ТЕХНОЛОГІЇ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІДПОВІДНО ДО ВІТЧИЗНЯНИХ НОРМАТИВНИХ ДОКУМЕНТІВ ТА МІЖНАРОДНИХ СТАНДАРТІВ

I.L. Obertuniyk, H.V. Karelina Ph.D, Assoc. Prof.

TECHNOLOGIES OF ASSESSMENT OF INFORMATION SAFETY RISKS IN ACCORDANCE WITH DOMESTIC NORMATIVE DOCUMENTS AND INTERNATIONAL STANDARDS

У світі інформаційних технологій та наукових досліджень поняття живучості відоме як властивість, яка характеризує здатність інформаційно-телекомунікаційної системи ефективно функціонувати за умови впливу чинників дестабілізації: збої в роботі, руйнування, компрометація тощо та відновлювати таку здатність протягом заданого проміжку часу. Аналіз і управління інформаційними ризиками - один з базових пропроцесів, що визначають ефективність системи забезпечення інформаційної безпеки організації. Оцінка ризику полягає у визначенні його рівня (якісної або кількісної величини) і порівнянні цього рівня з максимально допустимим (прийнятним) рівнем, а також з рівнем інших ризиків. Рівень ризику визначається шляхом комбінування двох величин: ймовірності події та розмірів його наслідків. При дослідженні алгоритмів для оцінки інформаційних ризиків ми розробили свій для підприємства «Укртелеком». Вхідними даними будуть: доступ до інформації, критичність доступу до інформації, вразливості, ймовірність реалізації загрози через певну вразливість, критичність реалізації загрози. Алгоритм передбачає два режими роботи коли існує одна базова загроза та коли є три базові загрози. В ньому розглядаємо одну базову загрозу. Для роботи з алгоритмом використано шкалу від 0 до 100 %, яку можна розбити на 100 частин. Кожна частина займає певний інтервал. Розбиття можна провести рівномірно та логарифмічно. На першому етапі роботи алгоритму розраховують рівень загрози за вразливістю *Th* на основі критичності та ймовірності реалізації загрози через цю вразливість. Рівень загрози передбачає, наскільки критичним є вплив цієї загрози на базу з врахуванням ймовірності її реалізації.

$$Th = \frac{ER}{100} * \frac{P(V)}{100}, \quad (1)$$

де *ER* – критичність реалізації загрози *(у %), P(V)* – ймовірність реалізації загрози через цю вразливість *(у %), Th* – рівень загрози за вразливістю.

Другий етап передбачає розрахунок рівня загроз за всіма вразливостями *CTh* , через які можлива реалізувувати цю загрозу на підприємстві. Підсумуємо отримані рівні загроз через конкретні вразливості за такою схемою:

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th_i), \quad (2)$$

де *CTh* – рівень загрози за всіма вразливостями, *Th* – рівень загрози за вразливістю.

Значення рівня загрози за всіма вразливостями має знаходитись у межах від 0 до1.

На третьму етапі аналогічно розраховуємо загальний рівень загроз за доступом до інформації *CThR* (враховуючи всі загрози, що впливають на базу)

$$CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i), \quad (3)$$

де *CThR* – загальний рівень загроз на базу, *CTh* – рівень загрози за всіма вразливостями.

На четвертому етапі ризик за доступом *R* розраховують так:

$$R = CTh * D \quad , \tag{4}$$

де R – ризик за доступом, $CThR$ – загальний рівень загроз за доступом, D – критичність доступу.

Критичність доступу визначають за такою формулою:

$$D = D_t * T \quad , \tag{5}$$

де D_t – критичність доступу за загрозою доступності на годину, T – максимально критичний час простою доступу.

На п'ятому етапі ризик за ІС CR розраховують за формулою:

Для режиму роботи в рівнях:

$$CR = \left(1 - \prod_{i=1}^{n}\left(1 - \frac{R_i}{100}\right)\right) * 100 \tag{6}$$

де CR – ризик за ІС, R – ризик за доступом.

Для оцінки ризику високого рівня, щоб визначити ризики, рівень яких вище прийнятного. Для визначення ризику необхідно визначити цінність інформаційного активу, вірогідність загрози та рівень вразливості я використовую стандарт в якому пропонується матриця зумовлених значень ISO/IEC 27005:2015[1], і порівнюю його з НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [2] складаю перелік загроз, описую методи та способи їх реалізації, для створення моделі загроз. При оцінці готовності вразливості, через яку може реалізуватися загроза, враховуються зручність (можливість) використання вразливості джерелом загроз, складність використання, необхідні кошти, можливість застосування неспеціалізованої апаратури. Тому при аналізі різних технологій оцінки і порівнюючи стандарти міжнародних і вітчизняних документів а також прирівнюючи різні аспекти організації я вважаю що краща технологія для оцінки ризику буде CRAMM. Тим що дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат і також має базу знань по ризикам і видам їх мінімізації, засоби збору інформації, формування звітів, а також реалізує алгоритм для визначення величини ризику. Метод пропонує всі процедури методу поділити на три послідовних етапи. У метод CRAMM закладено широкий набір типових рекомендацій щодо проведення контрзаходів для зменшення ризиків ІБ ІТС, але її ефективне використання можливе тільки фахівцями вищої кваліфікації.

В нашому дослідженні розглядається варіант новизни використання якісних величини з використанням різних додаткових умов тобто деякі загрози ІБ можуть ставитися відразу до кількох активів і навпаки - для одного активу можуть існувати кілька загроз різних класів. В роботі показані відмінності між ризиками і при цьому використовуються відповідні значення вартості активу в якості величини збитку і, внаслідок цього, для кожного активу розглядаються три різних ризику ІБ. Під технічним ризиком ми розуміємо значення ризику інформаційної безпеки, що складається з ймовірностей реалізації загроз і використання вразливостей кожного компонента інформаційної інфраструктури з урахуванням рівня їх конфіденційності, цілісності та доступності.

Література:

1.ISO/IEC 27005:2015 Інформаційні технології – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912

2.НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» - Режим доступу: http://www.dut.edu.ua/uploads/l_1023_75718671.pdf.