УДК 004.056

ПІДХІД ДО КОМБІНАЦІЇ МЕТОДУ CRAMM З МЕТОДОМ CVSS ДЛЯ ПОКРАЩЕННЯ ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПАНІЇ

Магдаліна М.І.
Науковий керівник – доцент Снігуров А.В.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
тел. +38(097) 933-78-40

The report presents a proposal for improving the methodology CRAMM for assessing information security risks, taking into account the solutions presented in the methodology for assessing the vulnerabilities of the CVSS. The improvement consists in modernizing the procedure for calculating the level of vulnerability by adding the parameters of the basic metric of the CVSS methodology. This will significantly increase the accuracy of information security risk calculations when building the company's information security management system.

При оцінці ризиків інформаційної безпеки (ІБ) компанії виникає питання якості такої оцінки. Якість оцінки ризику ІБ, по-перше, залежить від точності вихідних даних, до яких відносяться точність описання бізнес процесів компанії, розуміння ТОП-менеджментом компанії того, які активи в компанії реально критичні, точності опису моделі загроз, розуміння своїх вразливостей. А, по друге, від точності опису параметрів ризику ІБ – рівня (частоти) загроз, рівня вразливості, вартості критичного інформаційного активу.

Одним з кращих методів оцінки ризику ІБ є метод CRAMM (CCTA Risk Analysis and Management Method). Даний метод на даний час використовується в урядових департаментах Великобританії та прийнятий багатьма комерційними організаціями та іншими державними адміністраціями по всьому світу [1].

Рівень загрози в методі CRAMM оцінюються за п’ятибальною шкалою: дуже низький, низький, середній, високий або дуже високий. Зміст даної оцінки має такі значення: дуже низька - очікується, що інцидент траплятиметься в середньому не частіше одного разу на 10 років; низька - очікується, що інцидент траплятиметься в середньому раз на 3 роки, середня - очікується, що інцидент траплятиметься в середньому раз на рік, висока - очікується, що інцидент траплятиметься в середньому раз на 4 місяці, дуже висока - очікується, що інцидент траплятиметься в середньому раз на місяць.

Рівні вразливості оцінюються за шкалою низький, середній або високий. Зміст даної оцінки має такі значення: низька - якщо інцидент трапиться, ймовірність реалізації найгіршого сценарію (оцінено під час

оцінки активів) буде не більше 33%, середня - якщо інцидент трапиться, існуватиме від 33% до 66% шансів реалізації найгіршого сценарію (оцінено під час оцінки активів), висока - якщо інцидент трапиться, ймовірність реалізації найгіршого сценарію (оціненого під час оцінки активів) буде вище 66%.

Оцінка рівня активу здійснюється по кільком категоріям, як то «Менеджмент і бізнес-операції», «Особиста безпека», «Персональна інформація», «Юридичні та нормативні зобов'язання», «Правозастосування», «Комерційно-економічні інтереси», «Фінансові втрати/переривання діяльності». Рівень активу для кожної з цих категорій визначається в шкалі від 1 (мінімальний вплив на бізнес-процеси компанії) до 10 (максимальний вплив на бізнес-процеси компанії).

Результат оцінки ризику відповідно методу CRAMM розраховується в шкалі від 1 до 7. Можна побачити, що точність оцінки рівня загрози середня (п'ять рівнів), точність оцінки вартості активу висока (10 рівнів), але точність оцінки рівня вразливості нижче ніж середня (3 рівня). Зрозуміло, що цю методику розробляли фахові експерти, які вирішили визначити такі рівні показників ризику ІБ.

Виникає питання, як можна підвищити точність оцінки ризику ІБ? В доповіді пропонується рівень вразливості оцінювати відповідно методу CVSS. В стандарті NIST CVSS v3 критичність вразливостей оцінюється на основі декількох глобальних груп метрик: базові метрики, тимчасові метрики, метрики навколишнього середовища – дозволяють деталізувати базові та тимчасові метрики та врахувати особливості середовища в якому знаходиться вразливість, що підлягає оцінці.

Якщо використовувати як оцінку рівня вразливості для методу CRAMM базові метрики методу CVSS, то вже в дану метрику входять такі параметри, як Вектор доступу (Attack Vector), Складність атаки (Attack Complexity), Обов'язкові привілеї (Privileges Required), Взаємодія з користувачем (User Interaction), рівень збитків конфіденційності, цілісності та доступності інформації. Рівень вразливості згідно методу CVSS розраховується в шкалі від 1 до 10. В доповіді представлений механізм перерахунку рівня такої кількісної оцінки вразливості в якісну шкалу для використання в методі CRAMM, а також приклад оцінки ризиків ІБ для навчальної ситуації з використанням удосконаленого методу CRAMM.

Список використаних джерел:

1. CRAMM (CCTA Risk Analysis and Management Method) [Електронний ресурс]. – Режим доступу до ресурсу: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.

2. Common Vulnerability Scoring System [Електронний ресурс]. – Режим доступу до ресурсу: https://www.first.org/cvss/.