УДК 004.021
Ю.О. Тлустий
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ДОСЛІДЖЕННЯ МЕТОДІВ ВИРІШЕННЯ ЗАДАЧ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПРИ ВИКОРИСТАННІ БІЗНЕС-РІШЕНЬ

Y.O. Tlustiy

RESEARCH METHODS SOLVING PROBLEMS ASSESSMENT INFORMATION SECURITY THREATS WITH THE USE BUSINESS SOLUTIONS

Задача дослідження загроз безпеки інформації поділяється на дві стадії: ідентифікацію загроз; оцінку загроз.

Задача оцінки загроз передбачає:

– визначення методу оцінки загроз, причому оцінка, в свою чергу, може бути якісною і кількісною;

– оцінку наслідків інцидентів інформаційної безпеки;

– визначення характеристик ймовірності (випадковості) інцидентів інформаційної безпеки;

– обчислення рівня загроз.

Необхідно визначити, які підходи до оцінки загроз використовувати – якісні або кількісні. Враховуючи, що призначенням дослідження загроз є обґрунтування виділення фінансових коштів на заходи з обробки загроз, основним критерієм має бути ступінь корисності результатів для обґрунтування таких вкладень [1, 2].

Таким чином, з одного боку, якісні методи прості для розуміння і використання, з іншого – якісні методи не дозволяють дати конкретну оцінку, наскільки вигідне застосування комплексу контрзаходів і чи вигідно взагалі. До них відносять OCTAVE, PRo Audit Advisor і їм подібні.

У свою чергу, за допомогою кількісних методів можна із заданою точністю наголосити про необхідні засоби та заходи захисту, а також про ступінь економії коштів при їх впровадженні. У той же час існуючі методи і засоби мають ряд недоліків.

Розглянемо чотири підходи до кількісної оцінки загрози [3, 4]:

а) статистичні методи – передбачається визначення ймовірності реалізації загрози для розглянутого інформаційного активу за інтервал часу на основі виконання наступних вимог: об'єкти, до аналізу яких передбачається використовувати статистику, і об'єкти, на яких зібрана статистика, є еквівалентними (вимога еквівалентності об'єктів); умови, при яких передбачається використовувати статистику, і умови її збору є еквівалентними (вимога еквівалентності умов); обсяги вибірок статистики є достатніми, методи обробки – коректними, а джерела відомостей – заслуговують довіри (вимога переконливості).

До недоліків цієї групи методів слід віднести критичність до вихідних даних, які, як правило, або відсутні, або їх недостатньо для побудови коректних висновків.

б) ймовірнісно-статистичні методи використовують залучення додаткової інформації про розподіл збитків у разі реалізації загрози безпеці інформаційного активу. Передбачається, що для розглянутих умов функціонування організаційно-технічної системи підприємства відома функція розподілу збитку інцидентів інформаційної безпеки. На її основі визначається частка катастрофічних подій від загального числа негативних подій. Вважаючи цю частку постійною або прогнозуючи з тимчасового ряду її значення на заданий момент часу, можна визначити ймовірні характеристики катастрофічних подій. При цьому точність і достовірність результатів,

отриманих із застосуванням ймовірнісно-статистичних методів, визначається якістю і обсягом додаткової інформації про розподіл збитків.

в) теоретико-ймовірнісні методи використовуються для визначення частот або ймовірностей реалізації рідкісних загроз безпеці інформації зі значними наслідками, за якими статистика практично відсутня. В основі цього методу лежать закономірності переростання ініціюючих подій в надзвичайні, декомпозиція задачі, оцінки приватних показників і визначення частоти рідкісних негативних подій з урахуванням взаємозв'язку приватних показників.

Теоретико-імовірнісний метод досить трудомісткий, має низьку точність і достовірність отримуваних в процесі дослідження результатів, але при відсутності інших оцінок його застосування виправдане.

г) експертні методи ґрунтуються на знаннях і досвіді експертів. Ці методи доцільно застосовувати в тому випадку, коли відсутні статистичні дані. При цьому експертам пропонується відповісти на питання про стан або майбутню поведінку інформаційних активів, що характеризуються невизначеними параметрами або невивченими властивостями. Для інтерпретації або математичної обробки експертних даних можна використовувати математичний апарат теорії нечітких множин.

Складність аналізу загроз безпеки інформації експертним методом пов'язана, насамперед, з невизначеністю характеристик масивів даних, на базі яких сформовано досвід експерта і, як наслідок, з відсутністю гарантій отримання достовірних результатів.

Таким чином, можна констатувати наявність істотних обмежень у застосуванні відомих методів кількісної оцінки загроз у сфері безпеки інформації, у зв'язку з чим пошук нових підходів, які забезпечують вирішення задач визначення характеристик ймовірності (випадковості) безпеки інформації в умовах недостатніх статистик, являє собою актуальну задачу [5, 6].

Література.

1. Дослідження компанії KRC Research [Електронний ресурс]. - Режим доступу URL: http://www.krcresearch.com/selectReports.html.

2. ISO/IEC 27001:2005 “Information technology - Security techniques - Information security management systems - Requirements”.

3. Галицкий А. Защита информации в сети - анализ технологий и синтез решений. - ДМКПресс, 2004. - 615 с.

4. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. / С. А. Петренко, С. В. Симонов - М.: Компания Айти; ДМКПресс, 2004. - 653 с.

5. RiskWatch Обзор продукта [Електронний ресурс]. - Режим доступу URL: http://www.riskwatch.com.

6. ГРИФ Обзор продукта [Електронний ресурс]. - Режим доступу URL: http:// www.dsec.ru/soft.