РОЗШИРЕННЯ ПОНЯТТЯ РИЗИКУ В ТЕОРІЇ ЗАХИСТУ ІНФОРМАЦІЇ

Андрій Дудатьєв[1], Юрій Баришев[2]

Вінницький національний технічний університет
Хмельницьке шосе, 95, Вінниця, 21021, Україна, тел.: (0432) 59-84-85,
E-mail: [1]andreysaf60@mail.ru, [2]yura.baryshev@gmail.com

Анотація

В доповіді розглянуто місце ризику в теорії захисту інформації та його значення при проектуванні системи захисту інформації. Зроблено аналіз сучасного розуміння ризику, на основі якого визначено ряд недоліків, які полягають в тому, що сучасне поняття ризику не враховує специфічні властивості інформації. Відповідно було запропоновано шляхи усунення визначених недоліків.

Крім того, було запропоновано відокремлювати ризики відповідно до направленості атак стосовно інформаційних ресурсів з метою підвищення достовірності результатів експертного оцінювання ймовірностей успішних реалізацій атак на інформаційні ресурси. Були наведено математичну модель, яка дозволяє врахувати запропоновані підходи для визначення інтегрального ризику.

Було наведено приклад використання даних підходів. Викладений матеріал було узагальнено у висновках та було визначено перспективи подальшого дослідження.

Вступ

В межах рішення проблеми забезпечення інформаційної безпеки виникає задача оцінювання захищеності інформаційних ресурсів. Оцінювання інформаційної безпеки дозволяє визначити найслабші ланки, що входять до складу об'єкта дослідження, а також прогнозувати ефективність впровадження тих чи інших засобів та заходів захисту. В результаті оцінювання інженеру бажано отримати оцінки цих ресурсів, виражені у фінансовій формі, оскільки йому необхідно визначити суму коштів, які варто витрачати на удосконалення існуючої або проектування нової системи захисту інформації. Таким показником є ризик.

Сучасне розуміння ризику

Зазвичай ризик, пов'язаний з деяким інформаційним ресурсом, визначають так [1]:

$$R = P \cdot C, \tag{1}$$

де R – ризик;
P – ймовірність реалізації загрози на даний ресурс;
C – вартість максимальних збитків власника ресурсу від успішної реалізації атаки на цей ресурс.

У якості останнього показника, в більшості випадків, використовують вартість самого ресурсу. Якщо ж втрата даного ресурсу приводить до зупинки виробничого процесу, то в якості вартості максимальних збитків використовують збитки, спричинені цим простоєм, та вартість самого ресурсу. В конкретних випадках можуть різнитися підходи до визначення типів цієї вартості, але всіх їх можна формалізувати у такому вигляді:

$$C = \sum_{i=1}^{q} C_i, \tag{2}$$

де C_i – вартість і-тих збитків власника від успішної реалізації атаки на ресурс; q – кількість видів збитків власника.

Даний підхід до розрахунку ризиків може бути ефективними, якщо мова йде про фізичні ресурси. У випадку, коли необхідно оцінити саме інформаційні ресурси, можуть виникнути проблеми в його застосуванні, пов'язані зі специфікою безпосередньо інформації.

В літературі, пов'язаній з теорією захисту інформації [2], виділяють такі основні її характеристики:

- цілісність – характеристика безпеки інформації, що відображає її здатність протистояти несанкціонованій модифікації;
- доступність – характеристика безпеки інформації, яка відображає її властивість, що полягає у можливості використання відповідних ресурсів у заданий момент часу згідно пред'явлених повноважень;
- конфіденційність – характеристика безпеки інформації, що відображає її властивість нерозкритості та доступності без відповідних повноважень. Іншими словами конфіденційність – це "прихованість" інформації від осіб, які не мають права доступу до неї.

Таким чином, якщо порушується перша характеристика, то можна визначити вартість збитків власника даної інформації від такої атаки за формулою 2. У випадку, коли порушується доступність, то збитки також несе власник і їх також можна врахувати, але в зв'язку з тим, що дані збитки мають інший характер, ніж збитки, отримані від втрати цілісності інформації, для більш достовірних результатів їх варто формалізувати.

Часто ж в зловмисникам необхідно лише ознайомитися із засекреченою інформацією, наприклад, із виробничим ноу-хау, яке дозволяє його власнику виготовляти унікально кращу продукцію, ніж конкуренти. Якщо ж відбулася тільки втрата конфіденційності інформації, яка захищається, то виникає складність визначення розмірів збитків, які зазнав власник. Дана складність лише зростає у випадку, коли попит на цю унікальну продукцію на певному ринку вище за пропозицію, оскільки прямих збитків одразу власник не зазнає – ринок забезпечуватиме реалізацію продукції в повному обсязі без зміни ціни на неї. Отже одразу, після успішної реалізації зловмисником атаки, власник інформації збитків не зазнав.

Але в той же час зловмисник, який ознайомився з даною інформацію зможе також виготовляти цю унікальну продукцію та реалізовувати її на ринку, підвищуючи власні виробничі можливості. Через певний проміжок часу, коли ринок насититься даною продукцією і попит на неї спаде, власник інформації отримає серйозного конкурента на ринку в особі зловмисника, який колись дізнався цей виробничий секрет. Саме тут власник і буде зазнавати збитків.

Постановка задачі

Підсумовуючи вищенаведені роздуми, можна зробити висновок, що актуальною задачею є розширення поняття ризику, яке б дозволило враховувати збитки власника від порушення конфіденційності інформації, представленої у вигляді інформаційного ресурсу, та інтегрувати їх в поняття загального ризику.

Розширення поняття ризику

Збитки власника інформаційного ресурсу, отримані від порушення конфіденційності інформації, складно оцінити навіть, використовуючи нечіткі множини, оскільки на кількість збитків впливає багато різних факторів. До таких факторів можна віднести ймовірність того, що в майбутньому власник продукції отримає нове ноу-хау, те, як ефективно зуміє впровадити у виробництво отримані відомості зловмисник. Причому в даному випадку важливим є і ряд економічних факторів таких, як рівень спеціалізації підприємства-власника інформації. В зв'язку з цим необхідно використовувати інший підхід для оцінювання вартості інформації, а відтак і ризику, ніж розрахунок збитків власника.

Для розв'язання цієї задачі авторами пропонується у якості вартості інформаційного ресурсу використовувати його вартість для зловмисника, оскільки прибуток, отриманий зловмисником, буде задавати збитки власнику інформації в майбутньому. Таким чином, формулу 2 можна уточнити з урахуванням даної пропозиції:

$$C = \sum_{i=1}^{q} C_i + \sum_{j=1}^{n} C_j \,, \tag{3}$$

де C_i – вартість і-тих збитків власника від успішної реалізації атаки на ресурс;

C_j – вартість j-того прибутку зловмисника від успішної реалізації атаки на ресурс;

q – кількість видів збитків власника;

n – кількість типів прибутку зловмисника.

Інтегральні збитки власника інформаційного ресурсу можна розраховувати за допомогою формули 3, але, як відзначалося вище, в результаті оцінювання інформаційної безпеки необхідно отримати значення ризику. Оскільки під час оцінювання інформаційної безпеки доводиться використовувати нечіткі оцінки загроз безпеці, то для підвищення адекватності результатів оцінювання, авторами пропонується розділяти ризики відповідно до їх направленості. Так пропонується розрізняти для кожного інформаційного ресурсу такі ризики:

- ризик, пов'язаний з порушенням цілісності;
- ризик, пов'язаний з порушенням доступності;
- ризик, пов'язаний з порушенням конфіденційності.

Згідно даної класифікації інтегральний ризик визначатиметься за формулою:

$$\widetilde{R} = \sum_{i=1}^{N} \left(\widetilde{R}_{ці} + \widetilde{R}_{\partial i} + \widetilde{R}_{кі} \right), \tag{4}$$

де $\widetilde{R}$ – нечітке значення інтегрального ризику об'єкту оцінювання;

$\widetilde{R}_{ці}$ – нечітке значення ризику, пов'язаного з порушенням цілісності, для і-того інформаційного ресурсу;

$\widetilde{R}_{\partial i}$ – нечітке значення ризику, пов'язаного з порушенням доступності, і-того інформаційного ресурсу;

$\widetilde{R}_{кі}$ – нечітке значення ризику, пов'язаного з порушенням конфіденційності, для і-того інформаційного ресурсу;

N – кількість інформаційних ресурсів підприємства.

Відповідно до запропонованого підходу формалізуємо процес розрахунку ризиків. Визначення ризику, пов'язаного з порушенням цілісності, для і-того інформаційного ресурсу, визначатимемо так:

$$\widetilde{R}_{цi} = \widetilde{P}^{ц}_{ami} \cdot \sum_{j=1}^{p_i} C_{ij} \ , \tag{5}$$

де $\widetilde{P}^{ц}_{ami}$ – нечітка оцінка ймовірності успішної реалізації атаки зловмисником на і-тий інформаційний ресурс, направленої на порушення цілісності;

C_{ij} – вартість j-тих збитків власника від реалізації атаки на і-тий інформаційний ресурс, направленої на порушення цілісності;

p_i – кількість видів збитків власника від реалізації атаки на і-тий інформаційний ресурс, направленої на порушення цілісності.

Аналогічним чином формалізуємо ризик, пов'язаний з порушенням доступності, для і-того інформаційного ресурсу:

$$\widetilde{R}_{\partial i} = \widetilde{P}^{\partial}_{ami} \cdot \sum_{j=1}^{k_i} \left(\Delta t_{ij} \cdot w_{ij} \right), \tag{6}$$

де $\widetilde{P}^{\partial}_{ami}$ – нечітка оцінка ймовірності успішної реалізації атаки зловмисником на і-тий інформаційний ресурс, направленої на порушення доступності;

Δt_{ij} – тривалість відновлення доступу j-того користувача до і-того інформаційного ресурсу;

w_{ij} – питомі збитки власника внаслідок відсутності доступу j-того користувача до і-того інформаційного ресурсу;

k_i – кількість користувачів, які потребують для своєї діяльності і-тий інформаційний ресурс.

В формулі 6 у якості користувача інформаційного ресурсу може розглядатися і автоматизований процес, невиконання якого спричинює збитки для об'єкта.

Для визначення ризику, пов'язаного з порушенням конфіденційності, для і-того інформаційного ресурсу, використаємо запропонований підхід:

$$\widetilde{R}_{кi} = \widetilde{P}^{к}_{ami} \cdot \sum_{j=1}^{s_i} C^{/}_{ij} \ , \tag{7}$$

де $\widetilde{P}^{к}_{ami}$ – нечітка оцінка ймовірності успішної реалізації атаки зловмисником на і-тий інформаційний ресурс, направленої на порушення конфіденційності;

$C^{/}_{ij}$ – вартість j-тих прибутків зловмисника від реалізації атаки на і-тий інформаційний ресурс, направленої на порушення конфіденційності;

s_i – кількість видів прибутків зловмисника від реалізації атаки на і-тий інформаційний ресурс, направленої на порушення конфіденційності.

Перепишемо 4 з урахуванням формул 5-7:

$$\widetilde{R} = \sum_{i=1}^{N} \left(\widetilde{P}^{ц}_{ami} \cdot \sum_{j=1}^{p_i} C_{ij} + \widetilde{P}^{\partial}_{ami} \cdot \sum_{j=1}^{k_i} \left(\Delta t_{ij} \cdot w_{ij} \right) + \widetilde{P}^{к}_{ami} \cdot \sum_{j=1}^{s_i} C^{/}_{ij} \right), \tag{8}$$

За допомогою 8 можна розрахувати значення інтегрального ризику для об'єкта оцінювання інформаційної безпеки. Причому такий підхід дозволяє спростити експертам задачу оцінювання ймовірності реалізації атак, внаслідок конкретизації об'єктів цього оцінювання, тобто самих атак.

Приклад застосування запропонованого підходу

Оскільки метою даної роботи є саме розширення поняття ризику, а не розрахунок ймовірностей появи загроз, тому будемо вважати, що ймовірність появи загроз вже розрахована, за допомогою відомих методів [3], наприклад дерев ризику-відмов, програмна реалізація якого представлена в [4].

Розглянемо підприємство, яке займається виготовленням пластикових вікон. Інформаційними ресурсами в нього є:

- фінансова інформація, представлена у вигляді електронних фінансових звітів;
- інформація стосовно будівництв, які плануються в регіоні, представлена у вигляді бази даних (БД) потенційних замовлень;
- програмне забезпечення автоматизованої лінії виготовлення вікон.

Припустимо, що на основі проведення інформаційного обстеження відповідно до [5] з урахуванням критеріїв оцінювання, взятими, наприклад, з [6], група експертів визначила оцінки. Для спрощення припустимо, що оцінки мають трикутну форму функції приналежності та будуть записані у форматі, запропонованому в [7]: (найбільш ймовірне значення; відхилення ліворуч; відхилення праворуч). Відповідно

найменше та найбільше значення мають функцію приналежності 0, а найбільш ймовірне значення – 1. Наведемо в табл. 1 показники стосовно даного підприємства.

Таблиця 1 – Оцінки ймовірностей успішної реалізації загроз

Об'єкт атаки	Оцінка ймовірностей успішної реалізації загроз			Фінансові показники			
	цілісності	доступності	конфіденційності	C_{ij},грн.	Δt_{ij},год.	w_{ij},грн./год.	$C_{ij}^{/}$,грн.
Фінансові звіти	0,4;0,02;0,02	0,2;0,02;0,02	0,6;0,02;0,02	10000	2	500	20000
БД потенційних замовлень	0,2;0,02;0,02	0,9;0,02;0,02	0,4;0,02;0,02	1000	4	50	25000
Програмне забезпечення	0,1;0,02;0,02	0,6;0,02;0,02	0,9;0,02;0,02	500	5	1000	0

В табл. 2 наведемо результати розрахунку ризиків згідно даних табл.1 та правил арифметичних операцій над нечіткими числами [7].

Таблиця 2 – Прогнозовані фінансові показники від успішної реалізації загроз

Об'єкт атаки	Ризик			
	цілісності	доступності	конфіденційності	загальний
Фінансові звіти	4000; 200; 200	200; 20; 20	12000; 400; 400	16200; 620; 620
БД потенційних замовлень	200; 20; 20	180; 4; 4	10000; 500; 500	10380; 524; 524
Програмне забезпечення	50; 10; 10	3000; 100; 100	0	3050; 110; 110
Всього за направленістю	4250; 230; 230	3380; 124; 124	22000; 900; 900	29630; 1254; 1254

Згідно табл. 2 значення ризику для даного підприємства знаходиться в межах [28376; 30884], з найбільш достовірним значенням ризику 29630 грн.

Висновки

В даній доповіді запропоновано новий підхід до визначення ризиків власника інформаційних ресурсів, виходячи з прибутків, отриманих зловмисником, внаслідок успішної реалізації атаки. Також запропоновано шлях використання цього розширеного поняття ризику в процесі оцінювання інформаційної безпеки, що дозволить отримати підвищення достовірності результатів внаслідок спрощення процесу експертного оцінювання ймовірностей успішної реалізації атак. В подальшому передбачається створення математичної моделі для впровадження запропонованого підходу в процес проектування систем захисту інформації.

Література

[1] Астахов А. М. Аудит безопасности информационных систем // Защита информации. Конфидент.– 2003. – №1. – С.63-67, №2. – С. 90-96.
[2] Корченко А.П. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: МК-пресс, 2006. – 316 с.
[3] Лужецький В.А., Дудатьєв А.В., Баришев Ю.В. Оцінка інформаційної безпеки підприємства // Вісник Черкаського державного технологічного університету. – 2005. – №1. – С. 50-53.
[4] Дудатьєв А.В., Баришев Ю.В. Редактор дерева ризику-відмов // Інформаційні технологій та комп'ютерна інженерія. – 2007. – №1. – С. 86-89
[5] Державний стандарт України ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. – К.: Держстандарт України, 1996. - 11 с.
[6] Нормативний документ системи технічного захисту інформації НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – К.: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. – 53с.
[7] Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. – Вінниця: Універсум-Вінниця,1999. – 320 с.