Архипов О.Є., Архипова Є.О. Ризиковий підхід до визначення обсягу оптимальних інвестицій у безпеку інформації / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность. Материалы XV Международной научно-практической конференции ИТБ-2015. (21 жовтня 2015 р., м. Київ). – К.: ИПРИ НАН Украины, 2015. – 250 с. – С.12-17.

***Архипов Олександр**, д.т.н., проф., проф. кафедри інформаційної безпеки НТУУ «КПІ»*

***Архипова Євгенія**, к.філос.н., доц. кафедри теорії та практики управління НТУУ «КПІ»*

РИЗИКОВИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ОБСЯГУ ОПТИМАЛЬНИХ ІНВЕСТИЦІЙ У БЕЗПЕКУ ІНФОРМАЦІЇ

Одними з перших дослідників, які здійснили теоретико-методологічне обґрунтування граничного обсягу інвестицій у безпеку інформації, є американські вчені Л. Гордон і М. Лоеб. Згідно із їхнім дослідженням, оптимальний обсяг інвестицій в систему захисту інформації (СЗІ) не може перевищувати 36,79% від величини максимальних втрат, які можуть виникнути в разі реалізації загроз інформації. Проте Гордон і Лоеб не довели повноту та достатність запропонованої ними системи аксіом, що зумовило появу чисельних доповнень та модифікацій, а отже й різних висновків щодо величини граничних інвестицій у СЗІ, які, за деякими роботами, могли перевищувати 100 % від величини максимально можливих втрат. Причиною таких розбіжностей є формально-апроксимативний спосіб побудови функції ймовірності порушення захищеності інформаційних ресурсів, який не дозволяє врахувати відомості про реальні механізми розвитку та реалізації інформаційних загроз і ризиків.

Звернемося до моделі, запропоновані для дослідження економіко-мотиваційних відносин, характерних для ситуації «атака-захист» в інформаційній сфері [1; 2]. Вважатимемо, що D – загальна вартість витрат атакуючої сторони А на реалізацію загрози T відносно деякого інформаційного ресурсу I, який належить стороні В; g – отриманий при цьому «виграш» атакуючої сторони А, величина якого обумовлюється цінністю ресурсу I для зловмисника. Збитки, яких зазнала в цій ситуації сторона В (власник ресурсу I), тобто вартість ресурсу з точки зору його власника, оцінюється ним як q, а загальна вартість реалізованого комплексу захисних заходів дорівнює c.

В загальному випадку ймовірність реалізації загрози T відносно деякого інформаційного ресурсу I є добутком ймовірність активації (виникнення) загрози відносно інформаційного ресурсу (P_t) та ймовірність успішного використання зловмисником вразливостей інформаційної системи, яка містить ресурс I (P_v):

$$P_T = P_t P_v . \quad (1)$$

Значення ймовірності P_v залежить від рівня захищеності інформаційної системи, який у свою чергу обумовлюється обсягом інвестувань *c* в СЗІ [1]:

$$P_v = \frac{q}{q + sc}, \quad (2)$$

де *s* – коефіцієнт, яким визначає рівень ефективності інвестувань *c* в СЗІ, причому чим більше значення *s*, тим нижче величина ймовірності успішної реалізації атак.

У разі відсутності цінної інформації в ІС ($q = 0$) ймовірність $P_v = 0$. Коли вартість *q* ресурсу *I* висока чи дуже висока, а витрати на СЗІ низькі ($q >> sc$), ймовірність $P_v \to 1$. Якщо власник ресурсу *I* адекватно враховує його цінність *q* та приділяє його захисту відповідну увагу, значення *q* і *sc* можуть виявитися співрозмірними, але при цьому завжди буде виконуватися вимога $0 < P_v < 1$. Припустимо, що при $s=0$ $P_v=1$, а вихідний інформаційний ризик $R_1 = P_t q$. Інвестування у СЗІ коштів у розмірі *c* (та їх раціональне використання) призводить до того, що ймовірність успішного використання вразливості стає меншою за 1, тобто $P_v<1$. Залишковий ризик в цьому випадку дорівнюватиме $R_T = P_t P_v q$, величина втрат, які вдалося попередити: $R_1 - R_T = P_t q - P_t P_v q = (1 - P_v) P_t q$, а відповідний «прибуток» $\Delta_R = R_1 - R_T - c =$ $= (1 - P_v) P_t q - c$. Замінюючи P_v його розгорнутим виразом (2), отримуємо:

$$-c + \frac{sc}{q + sc} P_t q = \Delta_R, \quad (4)=3$$

Діапазон можливих значень *c* раціонально обмежити діапазоном «розумних» інвестицій: $0<c< q(s–1)/s$, при цьому коефіцієнт $s > 1$. Досліджуючи співвідношення (3) на екстремум (вважаючи, що Δ_R є функцією змінної *c*), отримуємо вираз: $\frac{d\Delta_R}{dc} = \frac{s(q + sc) - s^2 c}{(q + sc)^2} P_t q - 1 = 0$, з умов виконання якого [1] визначаємо обсяг інвестицій c_{eff}, що забезпечує отримання найбільшого значення Δ_R:

$$c_{eff} = \frac{q}{s}(\sqrt{P_t s} - 1), \quad (6)=4$$

а також формули розрахунку значення ймовірності P_v і ризику R для оптимального обсягу інвестицій:

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_t s}}, \qquad R_T(c_{eff}) = P_v(c_{eff}) P_t q = q\sqrt{\frac{P_t}{s}}. \qquad (7)=5$$

Аналіз формули (4) дає можливість оцінити максимальний обсяг інвестувань в СЗІ. Досліджуючи на екстремум залежність (4) як функцію змінної *s*, отримуємо:

$$\frac{dc_{eff}(s)}{ds} = q(s^{-2} - \frac{1}{2} s^{-3/2}\sqrt{P_t}) = 0. \qquad (8)=6$$

З рівності (6) знаходимо, що свого екстремуму функція $c_{eff}(s)$ досягає при значенні $s = 4/P_t$. Цьому значенню змінної *s* відповідає максимум функції $c_{eff}(s)$:

$$\max[c_{eff}(s)] = c_{eff}(4/P_t) = 0{,}25 q P_t. \qquad (9)=7$$

Очевидно, що найбільшою величина оптимальних інвестицій в СЗІ буде при P_t=1. Таким чином, максимальний обсяг оптимальних інвестицій в СЗІ дорівнює 0,25 вартості ресурсу з точки зору його власника. Отриману умову можна вважати формалізацією принципу розумної достатності при побудові СЗІ. Зазначимо, що з досвіду побудови СЗІ значення $s \geq 10 \div 45$ [1], а для високоефективних рішень $s = 40 \div 60$. Тому відповідно до формули (4) навіть при P_t=1 обсяг інвестицій в СЗІ може дорівнювати 11-13 % вартості ресурсу, що захищається.

Вираз (2) формує оцінку ймовірності успішного використання зловмисником вразливостей інформаційної системи головним чином на основі «внутрішніх» уявлень організації-власника ресурсу *I* (сторона В) про необхідний рівень захищеності цього ресурсу. Однак реальний ступінь захищеності ресурсу *I* значною мірою визначається інтенсивністю і силою атак сторони А, що залежать від її уявлень про цінність ресурсу *I*, тобто від величини *g*. Тому, якщо атакуюча сторона А точно ідентифікована і для неї достовірно відома величина *g*, можливо більш об'єктивною оцінкою ймовірності P_v є:

$$P_v = \frac{g}{g + sc}. \qquad (8)$$

За однакового розуміння цінності інформації сторонами А і В *g*=*q*. Але зазвичай ці сторони мають асиметричні уявлення про цінність інформації, що потребує вибору формули (2) чи (8). Для власника ресурсу *I* його цінність *q* зазвичай розраховується на основі аналізу вартісних аспектів створення цього ресурсу. Для атакуючої сторони А цінність *g* «добутої» інформації формується на основі ринкової вартості ресурсу *I* та кількості потенційних покупців, що бажають його придбати. Також «добута» стороною

А інформація може бути інформацію з обмеженим доступом (ІзОД), витік якої може завдати шкоди ряду третіх сторін, які пред'являтимуть претензії стороні В, як такій, що не забезпечила збереження ІзОД. Обсяг претензій у грошовому еквіваленті у цьому випадку і становитиме g [2], причому оцінювання g, на відміну від q, характеризується багатоваріантністю, нестійкістю та поганою прогнозованістю.

Припустимо, що $g \neq q$, причому стороні В, що захищається, відома оцінка вартості ресурсу з точки зору зловмисника. Тоді, з урахуванням формули (8) отримуємо для співвідношення (3) нову форму подання:

$$-c + \frac{sc}{g + sc} P_t q = \Delta_R, \tag{9}$$

а кінцеві вирази (4), (6) набудуть вигляду:

$$c_{eff} = \frac{q}{s}\sqrt{P_t s} - \frac{g}{s}, \tag{10}$$

$$\max[c_{eff}(s)] = c_{eff}(4g^2 / P_t q^2) = 0{,}25 q^2 P_t / g. \tag{11}$$

Найбільшою величина оптимальних інвестицій в СЗІ виявляється при $P_t = 1$ і складає $c_{eff\,\max} = 0{,}25q^2 / g$. Розбіжність g і q може стати причиною недостатнього або надлишкового інвестування в СЗІ. Для отримання об'єктивних даних про ***найбільшу*** величину оптимальних інвестицій в СЗІ у разі $g > q$ бажано користуватися формулою (8) і отримуваними на її основі співвідношеннями, тому окрім відомостей про рівень втрат q сторони В, необхідна інформація про цінність ресурсу I для атакуючої сторони А. У разі $g \leq q$ для оцінювання ***найбільшої*** величини оптимальних інвестицій в СЗІ слід використовувати співвідношення (7), враховуючи нестабільність отримуваних оціночних значень g. У зв'язку з цим цікавою є можливість застосування інших моделей, що описують альтернативні розглянутим імовірнісні параметри ризику.

Реалізація захисту інформації в організації можуть варіюватися у дуже широких межах, залежно від відношення організації до питань інформаційної безпеки (ІБ). Основним фактором, який визначає характер цих відносин, є ступінь (рівень) зрілості організації в аспекті ІБ [3]. Врахування цього фактору у формулі (2) здійснюється шляхом вибору значення коефіцієнта ефективності інвестицій s, зокрема, більш високому рівню зрілості організації відповідає більше значення s. Однак величина коефіцієнту ефективності інвестицій s залежить не тільки від поведінки сторони, що захищається В, але і від зусиль та цілеспрямованості дій атакуючої сторони А. Тому

адекватний вибір значення s виявляється дуже складним завданням. Спростити його можна, використовуючи основні фактори, що визначають потенціал атакуючої сторони, безпосередньо для обчислення імовірнісних параметрів P_t та P_v оцінки ризику. Зокрема, для представленого вище опису ситуації «атака-захист» отримуємо:

$$P_t = \frac{g - D}{g} = 1 - \frac{D}{g}. \qquad (12)$$

Змістовний аспект отриманої формули пояснюється так: чистий прибуток зловмисника у разі успішної реалізації загрози становить різницю між очікуваним «виграшем» g від використання (реалізації) отриманого ресурсу I та витратами D зловмисника на реалізацію цієї атаки. Якщо цінність ресурсу I для атакуючої сторони досить велика, то можна припустити, що зловмисник намагатиметься використати будь-які шанси для реалізації цієї загрози. Навпаки, якщо цінність ресурсу I для нього незначна, то економічні мотиви для виникнення загрози практично відсутні.

Для ймовірності P_v врахування ресурсних можливостей атакуючої сторони А здійснюється шляхом множення значення інвестицій c в знаменнику формули (2) на мультиплікатор c / D, що дозволяє врахувати інвестиції D, які здійснюються стороною А в реалізацію атаки:

$$P_v(c, D) = \frac{q}{q + s\dfrac{c^2}{D}}. \qquad (13)$$

Очевидно, що зростання витрат D обумовлює збільшення ймовірності P_v, тоді як збільшення інвестицій c у захист інформації дає протилежний ефект. Використання формул (12), (13) для обчислення ризику призводить до виразу виду:

$$R_T = P_t \frac{q}{q + s\dfrac{c^2}{D}} q = (1 - \frac{D}{g}) \frac{q^2 D}{qD + sc^2}. \qquad (14)$$

На жаль, застосування знайденого ризику (14) для подальшої реалізації оптимізаційної процедури не дозволяє отримати рішення у явному вигляді. Залежність $R_1 - R_T = (1 - P_v) P_t q$ після підстановки в неї виразу (14) набуває логістичного характеру, а аналіз нерівності $\Delta_R = R_1 - R_T - c \geq 0$ дає можливість лише визначити діапазон розумних інвестицій:

$$\frac{qP_t}{2}(1-\sqrt{1-\frac{4D}{sqP_t^2}}) \le c \le \frac{qP_t}{2}(1+\sqrt{1-\frac{4D}{sqP_t^2}}). \quad (15)$$

Потреба обчислення квадратного кореня у формулі (15) обумовлює очевидне обмеження $1 \ge 4D/sqP_t^2$, яке трансформується у нерівність виду $D \le 0{,}25sqP_t^2$, що накладається на обсяг інвестицій атакуючої сторони А. Крім того, зловмисник очікує отримати від викраденої інформації більше, ніж він витратив на її викрадення. Дослідження співвідношення (14) при D=0 показує, що максимальне значення розумних інвестицій в СЗІ не повинно перевищувати обсягу потенційних втрат q у разі викрадення ресурсу I. Зі збільшенням значень D, при $D \to 0{,}25sqP_t^2$ права і ліва межі діапазону (15) зближуються, при цьому в граничному випадку найбільша величина оптимальних інвестицій в СЗІ складе 0,5 вартості ресурсу з точки зору його власника.

Відзначимо, що наявність обмежень $D \le 0{,}25sgP_t^2$ і $g \ge D$ характерна для ситуації, коли атакуюча сторона А в своїх діях керується виключно принципом економічної доцільності (розумної достатності). Однак за певних обставин цей принцип може не виконуватися, зокрема у випадку виконання завдання найманим співробітником спецслужби, який у разі важливості поставленої перед ним задачі може розраховувати на широке залучення додаткових ресурсів: фінансових, технічних, інформаційно-аналітичних, оперативних. Якщо можливі витрати «зловмисника-виконавця» на отримання потрібного йому ресурсу практично нічим не обмежені, то ймовірність успішної реалізації атаки наближується до одиниці. В цій ситуації, якщо сторона, що захищається, створюючи свою СЗІ, виходить із принципу розумної достатності, ґрунтуючись виключно на власних («внутрішніх») уявленнях про цінність ресурсу I, успішна реалізація загрози атакуючої стороною А практично гарантована.

1. Архипов О.Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О.Є. Архипов, А.В. Скиба // Захист інформації. – 2013. – Том15, №4. – С.366 – 375.
2. Архипов О.Є., Архипова Є.О. Особливості визначення обсягу інвестицій в систему захисту інформаційних ресурсів / О.Є. Архипов, Є.О. Архипова // Інвестиції: практика та досвід. – 2015. – №11. – С. 71-74.
3. Петренко С. А Управление информационными рисками. Экономически оправданная

безопасность / С. А. Петренко, С. В. Симонов. – М. : Компания АйТи, ДМК Пресс, 2004. – 384 с.