

ПОРІВНЯННЯ МАТЕМАТИЧНИХ МОДЕЛЕЙ ІНВЕСТИВАННЯ В ІНФОРМАЦІЙНУ БЕЗПЕКУ ДЛЯ ВИРОБНИЧОЇ ІНФРАСТРУКТУРИ

О. І. Урсол¹, О. Є. Архипов¹

¹Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Фізико-технічний інститут

Анотація

В даній роботі було виконане порівняння математичних моделей інвестування в інформаційну безпеку для виробничої інфраструктури шляхом оцінювання за різними критеріями. Досліджено недоліки кожної з них та обрано найбільш кращу.

Ключові слова: інформаційна безпека, інвестування, математичні моделі

Вступ

В сучасних умовах економіки інформація є важливим нематеріальним активом підприємства. З розвитком Internet-технологій з'являється все більше і більше загроз безпеці інформації. Сьогодні питання гарантування інформаційної безпеки будь-якої організаційної інфраструктури, ефективно функціонування якої забезпечується масовим застосуванням інформаційних технологій, стає надзвичайно актуальним. [1]. Серед ключових факторів, що впливають на рівень інформаційної безпеки організації, експерти називають неправильне керування її бюджетом у питанні інвестування заходів з інформаційної безпеки, зокрема констатують існування потреби в більш детальному аналізі та дослідженні моделей оптимального інвестування в інформаційну безпеку та знаходженні ефективного розподілу обмежених фінансових ресурсів на захист інформації суб'єктів.

1. Основна частина

На формування економічної безпеки підприємства впливає зміна умов господарювання, які характеризуються нестабільністю та нестійкістю економічного середовища. Для цієї ситуації на поточний момент відсутня розроблена модель раціонального інвестування в інформаційну безпеку. Задача даної роботи — вибрати більш-менш підходящу математичну модель інвестування в інформаційну безпеку для довільної організаційної інфраструктури. На сьогодні однією з найбільш поширених і відомих моделей, що застосовуються для аналізу ефективності виконаних інвестувань в СЗІ, є модель, розроблена двома американськими дослідниками в області економіки Лоуренсом Гордоном і Мартіном Лоебом з університету Меріленд [2]. Інформаційний ресурс характеризується трьома параметрами: λ , $t \in [0, 1]$, і $\nu \in [0, 1]$, де λ — втрати, зумовлені порушенням захищеності інформації, t — ймовірність виникнення погрози, ν — вразливість, котра в моделі являється ймовірністю того, що реалізована загроза виявиться

успішною. Хоча λ залежить від використання інформації (самою організацією, конкурентами, хакерами) і змінюється в часі, в моделі вважається, що λ — фіксоване значення, кінцеве і менше деякого дуже великого числа M . Таким чином, модель не призначена для випадків захисту національних (державних) активів або будь-яких інших, де втрати можуть бути катастрофічними. Для катастрофічної втрати $\lambda \geq M$ припущення про нейтральність до ризику організації стає нереалістичним. Для заданого інформаційного ресурсу ймовірність втрати дорівнює νt , а очікувана втрата, обумовлена відсутністю інвестицій в ІБ, дорівнює $\nu t \lambda$. Таким чином, для будь-якої позитивної ймовірності загрози ($t > 0$) очікувана втрата зростає зі зростанням уразливості. Для даної моделі робиться спрощення, що організація може інвестувати в зменшення уразливості, але не може впливати на зменшення загроз. Тому ймовірність загроз $t > 0$ фіксується, і далі можна сфокусуватися на виборі обсягу інвестицій з метою зменшення вразливості. Оскільки $t = \text{const}$, визначається значення $L = t \lambda$ — втрати або потенційні втрати, пов'язані з інформаційним ресурсом.

З метою визначення кількості грошових коштів для інвестування в захищеність інформації, організація порівнює очікуваний прибуток від інвестицій із вартістю інвестицій. Очікуваний прибуток від інвестицій в інформаційну безпеку, позначений через $EBIS$, дорівнює зменшення очікуваних втрат організації, зумовленого додатковим захистом:

$$EBIS(z) = [\nu - S(z, \nu)]L. \quad (1)$$

Очікуваний чистий прибуток від інвестицій в інформаційну безпеку, позначена через $ENBIS$, дорівнює різниці $EBIS$ і вартості інвестицій:

$$ENBIS(z) = [\nu - S(z, \nu)]L - z. \quad (2)$$

Позначимо оптимальні інвестиції через $z^*(\nu)$. Для визначення оптимального рівня інвестицій в ІБ вирі-

шується завдання пошуку максимуму функції:

$$ENBIS = (z) = ENBIS(z^*) = \max_z [\nu - S(z, \nu)]L - z. \quad (3)$$

Вище зазначена економічна модель Городона-Лосеба показує, що оптимальний рівень інвестицій не перевищує $1/4 \approx 36,8\%$ від розміру збитку внаслідок порушення безпеки інформаційного активу.

Модель Архипова. В [3] для визначення необхідних імовірнісних параметрів запропоновано використовувати певні характеристики мотиваційно-вартісних та економіко-фінансових відносин, характерних для ситуації «атака-захист» в інформаційній сфері. Зокрема, розглянуто ситуацію, що виникає при реалізації атакуючою стороною А (зловмисник) загрози Т відносно деякого інформаційного ресурсу І, який належить стороні В. Для опису ситуації введено наступні позначення [3]:

- загальна вартість витрат атакуючої сторони А на реалізацію загрози Т;
- «виграш», отриманий атакуючою стороною А, величина якого обумовлюється цінністю ресурсу І для атакуючого;
- збитки, яких зазнала в цій ситуації сторона В (вартість/цінність/важливість критичної інформації з точки зору її власника – сторони В);

Чистий прибуток атакуючої сторони А в разі успішної реалізації загрози визначається за формулою:

$$Q = g - D. \quad (4)$$

Виходячи з мотиваційних характеристик зловмисника (сторона А), вважаючи, що він діє виключно за принципом економічної доцільності, можливі такі варіанти:

- 1) якщо $g \gg D$, вважається, що ймовірність P_t виникнення загрози Т буде практично дорівнювати 1, тобто атакуюча сторона А спробує використати будь-які шанси для реалізації цієї загрози;
- 2) для малих значень g економічні мотиви виникнення загрози практично відсутні: при $Q = 0$ (або $g = D$) атака ресурсу І стає недоцільною, в цьому випадку $P_t = 0$;
- 3) для $g < D$ спроба реалізації загрози Т втрачає будь-який економічний сенс.

Виходячи з цих міркувань, для оцінювання значень імовірності виникнення загрози Т запропоновано співвідношення:

$$P_t = \frac{Q}{g} = 1 - \frac{D}{g}. \quad (5)$$

Для оцінки імовірності P_t виникнення загрози враховуючи рівень індивідуальних мотиваційних характеристик зловмисника використано формулу:

$$P_t = \frac{\gamma g - D}{\gamma g} = 1 - \frac{D}{\gamma g}. \quad (6)$$

де коефіцієнт мотивації γ відображає ступінь впливу величини «виграшу» g на дії атакуючої сторони А (зловмисника). Для впевненого в собі зловмисника $\gamma > 1$, для обережного – $\gamma < 1$.

Імовірність P_v успішного проведення комплексу атак, породжених існуванням сукупності вразливо-

стей інформаційної системи (включно із вразливостями самої системи захисту інформації), залежить від величини витрат D атакуючої сторони А на реалізацію загрози Т та ступеню захищеності інформаційної системи, який в першу чергу зумовлюється величиною c – обсягом інвестувань в систему захисту інформації:

$$P_v = \frac{q}{q + s \frac{c^2}{D}}. \quad (7)$$

де s – коефіцієнт, діапазон значень якого пов'язаний із залежністю між рівнем інвестицій c та цінністю критичної інформації (наприклад, для комерційної таємниці прийнято $c = (0,05 \div 0,20)q$, $s \geq 10 \div 85$).

Наведені вище формули пропонується застосовувати безпосередньо для обчислення ризиків будь-якої конкретної організації за умов, що існує реальна змога проаналізувати та кількісно оцінити економіко-вартісні характеристики реалізації загрози інформації.

У статті [4] викладено підхід до вирішення проблеми інвестування системи захисту інформації в умовах обмежень на фінансові ресурси і розроблений алгоритм його реалізації на основі методів експертної оцінки, теорії ігор і математичного програмування. Отримане рішення базується на запропонованій моделі Глушака-Новікова, яка направлена на оптимальне розміщення механізмів захисту між компонентами (об'єктами) системи, що забезпечує мінімум ризику втрат інформації.

Пошук оптимального набору механізмів захисту пояснюється на прикладі системи районних відділень банку. Обсяг інформації в кожному відділенні пропорційний потенційній кількості клієнтів, тобто чисельності жителів району. Імовірність реалізації окремих загроз, а також вартість і ефективність кожного з механізмів захисту визначається методом експертної оцінки. При цьому припускається, що імовірність реалізації загрози проти кожного об'єкта однакова і залежить тільки від виду загрози. Розглядаючи різні комбінації елементів захисту для кожного з відділень, розраховується сумарний збиток для всієї системи (який і характеризує ступінь ризику) і оптимальний набір елементів захисту для кожного відділення за умови введення обмеження на загальну вартість системи захисту.

Цікаві рішення пропонуються у статті Б.Є. Журиленка [5, 6], де досліджується оцінка стійкості комплексу технічного захисту інформації (ТЗІ) в часі з використанням відомих розподілів ймовірностей. Імовірнісна надійність комплексу технічного захисту інформації визначається за виразом:

$$P_i(X_i) = \left(\frac{X_i X_i}{(1 + X_i)^{1+X_i}} \right)^{\beta_s}. \quad (8)$$

де $X_i = x_i/H_i$ – фінансові інвестиції у захист інформації; x_i – фінансові витрати на створення даного ТЗІ; H_i – початкові фінансові втрати за відсутності захисту; β – ефективність захисту залежно від фінансування.

Табл. 1. Критерії порівняння

Критерії порівняння	Моделі	Модель Гордона-Лоеба	Модель Глушака-Новікова	Модель Журиленка	Модель Архипова
Враховано ресурси захисту		+	+	+	+
Враховано ресурси нападу		—	—	—	+
Враховано вартість приблизних витрат ресурсів		+	—	—	+
Враховано ресурси на вартість відновлення системи		—	—	—	—
Враховано вартість окремого засобу захисту		—	+	—	+
Враховано уразливості об'єктів		+	—	+	+
Враховано вартість окремої частини системи		—	—	+	—
Адаптація моделі до конкретної реальної ситуації атака/захист		—	+	+	—
Враховано ступінь адекватності моделі характеристики реальної конфліктної ситуації		—	+	—	+
Оптимізація розподілу ресурсів між об'єктами захисту		—	+	—	—
Розрахунок оптимального рішення в динамічному режимі		—	—	+	+

Для визначення ефективності технічного захисту інформації необхідні експериментальні, сертифіковані або статистичні дані імовірності зламу даної системи захисту і час, коли настала така імовірність.

Імовірність зламу в часі визначається за формулою:

$$P_i(t) = \left(\left(\frac{t_0 i}{t_0 i + t} \right)^{\frac{t_0 i}{t}} \left(\frac{t}{t_0 i + t} \right)^{\gamma_i} \right). \quad (9)$$

де $t_0 i$ – часовий параметр, властивий даній системі захисту, і який може бути визначений лише внаслідок реальних результатів порушення безпеки; t – поточна координата часу; γ_i – визначає ефективність захисту в часі.

В результаті проведених досліджень показано, що t_0 – параметр, що визначає властивості ТЗІ, може бути не лише сталою величиною, а й функцією, що залежить від спроб зламу і від часу, коли такі спроби мають місце. На основі досліджень отримано функції, що дають можливість розрахувати частоту спроб зламу.

Узагальнення порівняльного аналізу описаних вище математичних моделей інформаційної безпеки за системою уведених бінарних характеристик (критеріїв порівняння) представлено таблицею 1. За цими даними очевидно, що використовуючи бінарну систему оцінок 0/1 (або +/–), виокремити однозначно найкращу модель не має змоги. Деталізація результатів порівнянь, наприклад, шляхом введення ваг окремих критеріїв, веде до суб'єктивізації кінцевого висновку. Теж саме стосується вибору діапазону вразливостей, на якому зосереджується вибір механізмів та ресурсів захисту.

Висновки

У роботі було проаналізовано математичні моделі оптимального інвестування в інформаційну без-

пеку виробничої інфраструктури. Найбільшу кількість плюсів (+) набрала четверта математична модель. Але вона все ж не відповідає деяким критеріям (табл. 1), вага яких за певних обставин може бути вирішальною. Очевидно, що отримані результати можуть зазнати змін, якщо враховувати такі фактори, як: поглиблення дослідження економічних аспектів інформаційної безпеки, застосування ширшого кола моделей оцінки обсягу оптимальних інвестицій в ІБ, модифікацію сукупності (вектора) критеріїв порівняння та вибору діапазону вразливостей, на якому зосереджуються механізми та ресурси захисту. Тому продовження дослідження слід спрямувати у напрямку розробки методики оцінки оптимального рівня інвестицій, інваріантної до наведених вище факторів.

Перелік використаних джерел

1. Степко О. Н. Аналіз головних складових інформаційної безпеки держави[стаття]
2. Gordon L. The Economics of Information Security Investment / L. Gordon, M. Loeb — 2002 — 438-457
3. Архипов О. Є. "Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації"
4. Глушак В. В., "Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника" — Системні дослідження та інформаційні технології — 2013 — С. 89-100.
5. Журиленко Б. Е., Николаева Н. К., Пелих Н. С. "Оценка стойкости технической защиты информации во времени" 2014. — 104-108
6. Журиленко Б. Е. Математическая модель вероятностной надежности комплекса технической защиты информации // Безопасность информации.. — 2012 — 61-65