Олександр Архипов, Андрій Скиба
Національний технічний університет України «Київський політехнічний інститут»
УДК 004.056

ПРОБЛЕМАТИКА ВИЗНАЧЕННЯ ІНВЕСТИЦІЇ В ІНФОРМАЦІЙНУ БЕЗПЕКУ НА ОСНОВІ ЕКОНОМІКО-ВАРТІСНИХ МОДЕЛЕЙ

Антотація: **Розглянуто застосування економіко-вартісної моделі «атака/захист» для визначення обсягу інвестицій в систему захисту інформації організації, спрямованих на зменшення ризиків втрати інформації за умов раціонального розподілу загальних фінансових ресурсів організації та підвищення її інформаційної безпеки. На сьогоднішній день ситуація із розподілом ресурсів для розробки та реалізації заходів і засобів з інформаційної безпеки організації вимагає оновлення, бо результати попередніх досліджень та практичного застосування існуючих підхідів показали, що використання в них відомої моделі Гордона-Лоеба не дає змоги враховувати всі необхідні для правильного розподілу фактори. Це, зокрема, призводить до помилок при оцінці інформаційних ризиків, а відтак - до недоінвестувань в інформаційну безпеку. Проведене аналітичне порівння економіко-вартісної моделі з моделю Гордона-Лоеба дозволяє отримати об'єктивні висновки щодо застосовності цих моделей для оцінки інвестицій та їх ефективності. Модель Гордона-Лоеба має відверто формальний характер і не потребує для свого практичного застосування ніякої інформації про реальний стан захищеності інформації в організації. Запропонована економіко-вартісна модель завдяки прозорій стурктурі припускає просту та зрозумілу для фахівця у сфері захисту інформації інтерпретацію й дозволяє використовувати для свого практичного застосування реальні дані, отримані у процесі аналізу ризиків, забезпечуючи більшу об'єктивність та точність отриманих результатів. Задля забезпечення наглядності переваг запропонованої моделі, зроблено співставлення двох моделей у достатньо широкому діапазоні їх можливих застосувань.**
Summary: **In this article, the usage of economic-cost model of "attack/defense" to determime amount of information security investments is proposed. Information security investments are aimed to reduce the risk of information loss in conditions of rational distribution of total financial resources of the company and improve its information security. The current situation of resources, which are proveided for the development and implementation of measures and tools for information security organization requires updating, as the results of previous studies and practical implementation of the existing approach showed that the use of Gordon-Loeb model makes it impossible to consider all necessary factors for the proper distribution. In particular, it leads to mistakes in assessing information risks, and therefore - to underinvestment in information security. Conducted analytical comparison of economic-cost model "attack/defense" with models of Gordon-Loeb allowed to objective conclusions about usage of these models for assess investments and their effectiveness. Gordon-Loeb Model has openly formal nature and doesn't require its practical usage for any information about the real state of information security in the company. The proposed economic-cost model through a transparent structure is simple and understandable for experts in the field of information security and it's interpretation allows for practical exploitation to use f real data obtained in the process of risk analysis, which provides a greater objectivity and accuracy of the results. In order to ensure illustrative advantages of the proposed model, the comparison of the two models is made in quite wide range of possible usage.**
Ключові слова: **Інформаційна безпека, метод визначення обсягу інвестицій в інформаційну безпеку, інформаційна безпека компанії, економіко-вартісні моделі інформаційної безпеки.**

І Вступ

На поточний момент необхідність захисту інформації, а відтак, необхідність інвестування коштів в її безпеку, не викликає сумнівів. Однак необхідність інвестування, обсяги інвестицій та раціональний розподіл ресурсів не підкріплені нормативно-правовою документацією, відсутні відповідні настанови з боку регулятивних органів, що в свою чергу створює невизначеність для спеціалістів інформаційної безпеки в компаніях. За даними О. Лукацького, бізнес-консультанта Cisco з безпеки, більшість організацій (78% від обсягу всіх організацій, задіяних у дослідженнях) на заходи, пов'язані із безпекою інформації, витрачають не більше 15% від їх IT-бюджету, ще 11% організацій – від 16 до 20%, і лише 7% організацій – від 21 до 28% [1]. Характерно, що переважна більшість рекомендацій щодо обсягу інвестувань формується з подібних до наведеної вище довідок, тобто носить емпіричний характер, базуючись виключно на узагальненні досвіду розробки та експлуатації існуючих систем захисту інформації, або проведенні досліджень для державних та комерційних компаній. Саме це пояснює ту увагу, яку привернула до себе стаття американських дослідників в області економіки Лоуренса Гордона і Мартіна Лоеба [2], в якій на базі запропонованої ними економіко-математичної моделі зроблено спробу теоретико-методичного обґрунтування граничного обсягу інвестувань у

безпеку інформації. За даними Гордона та Лоеба [2] граничний обсяг інвестицій в інформаційну безпеку організації не має перевищувати 37% від максимального об'єму втрат, що їх нестиме організація у разі успішної реалізації щодо неї інформаційної загрози.

На жаль, для моделі Гордона-Лоеба та її численних розширень характерна суттєва вада: формально-апроксимативний спосіб завдання моделі, за яким майже повністю виключається можливість врахування при формування структури та параметрів моделі відомостей про реальні механізми розвитку і реалізації інформаційних загроз і ризиків, що суттєво обмежує практичні аспекти застосування означеної моделі. В цій ситуації інтерес представляють моделі, запропоновані в [3 – 7] для дослідження мотиваційно-вартісних та економіко-фінансових відносин, характерних для ситуації «атака-захист» в інформаційній сфері.

В нашому досліджені запропоноване удосконалення економіко-вартісної моделі з урахуванням сучасних нормативно-правових вимог до моделей, що використовуються для оцінки об'єму інвестицій в інформаційну безпеку.

II Огляд існуючих моделей для визначення інвестицій в інформаційну безпеку

Найпоширеніша у практичному застосуванні модель була запропонована американськими дослідниками Лоуренсом Гордоном і Мартіном Лоебом з університету Мєріленд у 2002 році, але, зазнавши ряд розширень і критики, автори оновили модель у 2015 році [8]. Розширення моделі Гордона і Лоеба – одноперіодична економічна модель: ризик-нейтральна фірма роздумує над тим, скільки інвестувати в інформаційну безпеку. Автори позначили через $S(z,v)$ функцію ймовірності порушення безпеки компанії, де z - інвестиції компанії в її інформаційну безпеку і v $(0 \le v \le 1)$ - ймовірність успішної реалізації атаки, що призведе до порушення інформаційної безпеки. Гордон та Лоеб в своїй новій публікації, як і в дослідженні 2002 року, припускають, що функція ймовірності порушення безпеки двічі неперервно диференційовна і задовольняє наступним п'ятьом регулятивним умовам: 1) для всіх $z \ge 0$, $S(z,0) = 0$; 2) для всіх $v \in (0,1)$, $S(0,v) = v$; 3) для всіх $v \in (0,1)$ і для всіх $z \ge 0$ і $\frac{\partial S(z,v)}{\partial z} < 0$; 4) для всіх $v \in (0,1)$ і для всіх $z \ge 0$, $\frac{\partial^2 S(z,v)}{\partial z^2} > 0$; 5) для всіх $v \in (0,1)$, $\lim_{z\to\infty} S(z,v) = 0$.

Тобто: 1) якщо інформація організації абсолютно невразлива, то ймовірність порушення безпеки залишиться на такому ж рівні для всіх обсягів інвестицій в інформаційну безпеку, тобто, якщо інформація абсолютно невразлива, то при будь-якому рівні інвестицій інформація залишається абсолютно захищеною, то ж рівень інвестицій не впливає на захищеність інформації, а відтак інвестиції є безмістовними; 2) якщо інвестиції в інформаційну безпеку відсутні, то ймовірність успішного порушення дорівнюватиме існуючій ймовірності можливого порушення або тій вразливості, яка відома організації в момент проведення оцінки (автори не дають пояснень на рахунок того, що відома ймовірність порушення є повною чи частковою); 3) збільшення інвестицій в інформаційну безпеку буде зменшувати ймовірність її успішного порушення; 4) функція ймовірності порушення безпеки є строго опуклою в z, тобто при збільшенні інвестицій ефективність засобів захисту спадає або ж залишається на тому самому рівні; 5) достатньо великий об'єм інвестицій в інформаційну безпеку може наблизити ймовірність успішного порушення як завгодно близькою до нуля.

Виходячи з п'яти регулятивних умов, Гордон і Лоеб при прийнятті рішення щодо інвестицій в інформаційну безпеку акцентують увагу на тому, що організація буде вибирати інвестиційний рівень (z^*) так, щоб отримати максимально повну вигоду від інвестицій в інформаційну безпеку:

$$max_z[v - S(z,v)]L^P - z. \quad (1)$$

Співвідношення (1) відповідає наступній умові:

$$-S_z(z,v)L^P = 1, \quad (2)$$

де z – інвестиції в інформаційну безпеку, L^P – втрати компанії від успішної реалізації атаки, v – вразливість інформації при успішній атаці, $S(z,v)$ – функція ймовірності порушення безпеки компанії.

В подальшому досліджені Гордон і Лоеб пропонують використати два класи функцій [9, 10], які на їх думку підходять найкраще для представлення ймовірності реалізації комплексної загрози організації.

В удосконаленій моделі 2015 року Гордон та Лоеб запропонували враховувати не тільки приватні втрати L^P організації (фірми, компанії), але і зовнішні або побічні втрати L^E, які є втратами покупців або партнерів організації і не стосуються приватних втрат. Загалом сукупні соціальні втрати для організації автори пропонують обраховувати як $L^{SC} = L^E + L^P$. Згідно з цією модифікацією формула для визначення інвестицій в інформаційну безпеку була оновлена до наступного вигляду:

$$max_z[v - S(z, v)]L^{SC} - z. \tag{3}$$

та відповідає наступній умові:

$$-S_z(z^{SC}, v)L^{SC} = 1. \tag{4}$$

Гордон і Лоеб пропонують ще деякі пояснення щодо використання їхніх формул і в результаті дослідження наводять оновлену формулу для визначення оптимальних інвестицій в інформаційну безпеку:

$$z^*(v) = \frac{\left[(v\alpha\beta L^P)^{\beta^1+1} - 1\right]}{\alpha}, \tag{5}$$

де початкова вразливість інформації при успішній атаці $v = 0{,}64$, параметри $\alpha = 0{,}00001$, $\beta = 1$, і приватні втрати компанії від порушення інформаційної безпеки становлять \$400,000. Потім за допомогою (5) оптимальними інвестиціями в інформаційну безпеку є інвестиції в об'ємі \$60000 (що дорівнюють 23,4375% від його очікуваного приватного збитку). Ефект зовнішніх втрат становить 5% від приватних втрат, або \$20000, згідно з цим сукупні соціальні втрати становитимуть \$420000. Використавши для обрахунку оптимальних інвестицій в інформаційну безпеку на основі сукупних соціальних втрат функцію L^{SC} автори встановили, що оптимальні інвестиції в інформаційну безпеку для компанії становлять \$63951. Таким чином, Гордон і Лоеб показують, що якщо розраховувати інвестиції в інформаційну безпеки виходячи тільки з приватних втрат, то компанія недоінвестує в інформаційну безпеку значну частину, бо не враховує зовнішні втрати від успішної реалізації загрози, тому більш коректною оцінкою буде оцінка інвестицій в інформаційну безпеку на основі приватних та зовнішніх втрат.

Слід однак зазначити, що для моделі Гордона і Лоеба характерні певні вади. Головна з них – жодним чином не доведено адекватність застосування обраних в [2, 8] класів функцій для оцінки інвестицій в інформаційну безпеку, наприклад, відсутнє співставлення розрахункових модельних даних із точковими оцінками ймовірностей реалізації загроз, отриманими з реальної статистики інцидентів в сфері захисту інформації. У своєму дослідженні Гордон і Лоеб зупинилися на функції (6) аж ніяк не інтерпретуючи цей вибір через реалії компанії, зокрема, оцінки інформаційних ризиків, актуалізацію ситуації через аналіз множини можливих загроз, атак, пошук потенційних каналів витоку інформації, виявлення ймовірних інсайдерів серед співробітників тощо:

$$S^I(z, 0, 64) = \frac{0{,}64}{0{,}00001z + 1}. \tag{6}$$

Певною альтернативою моделі Гордона і Лоеба є економіко-вартісна модель [4] оцінки інвестицій в інформаційну безпеку. Для її кращого розуміння розглянемо ситуацію, що виникає при реалізації атакуючою стороною А (зловмисник) загрози T відносно деякого інформаційного ресурсу I, який належить стороні B [11]. Вважатимемо, що D – загальна вартість витрат атакуючої сторони на реалізацію загрози, d – загальна вартість неочікуваних витрат зловмисника, що виникають до, в процесі або після реалізації атаки стороною A, g – отриманий при цьому «виграш», величина якого обумовлюється цінністю ресурсу I для ринку. Збитки, яких зазнала в цій ситуації сторона B (власник ресурсу I), тобто вартість ресурсу з точки зору його власника, оцінюється ним як $q_{sc} = q_p + q_s$, де q_{sc} – загальна вартість ресурсів компанії, q_s – соціальна вартість ресурсів компанії, q_p – приватна вартість ресурсів компанії, а загальна вартість реалізованого комплексу захисних заходів дорівнює c.

Наведені дані дають вартісну характеристику ситуації «атака-захист». На базі цих відомостей можна побудувати логіко-евристичну схему експертного оцінювання ймовірнісних характеристик, що використовуються для обчислення інформаційних ризиків та при комплексній оцінці інформаційних ризиків.

Чистий прибуток зловмисника в разі успішної реалізації загрози T складає $Q = g - (D + d)$. Якщо цінність ресурсу I для атакуючої сторони A значна, зокрема, якщо $g \gg D + d$, можна припустити, що зловмисник спробує використати будь-які шанси для реалізації цієї загрози. Навпаки, для малих значень g економічні мотиви виникнення загрози T практично відсутні: при $Q = 0$ (або ж $g = D + d$) атака ресурсу I стає недоцільною, в цьому випадку $P_t = 0$. Для $g < D + d$ спроба реалізації загрози T втрачає будь-який економічний сенс. Виходячи з цих міркувань, в [4] запропоновано співвідношення:

$$P_t = \frac{Q}{g} = 1 - \frac{D + d}{g}, \tag{7}$$

яке може бути використане для оцінювання приблизних (орієнтовних) значень ймовірності активації (виникнення) загрози T.

В загальному випадку ймовірність P_T реалізації загрози T – це добуток $P_T = P_t P_v$, де P_v – ймовірність вдалого використання зловмисником вразливостей інформаційної системи (ІС), що містить інформаційний ресурс I. Значення ймовірності P_v залежить від ступеню захищеності ІС, який в свою чергу зумовлюється обсягом інвестувань c в систему захисту інформації (СЗІ):

$$P_v = \frac{q_{SC}}{q_{SC} + SC}, \tag{8}$$

де c – коефіцієнт, пов'язаний з існуючою у світовій практиці залежністю між рівнем інвестицій c у захист та цінністю критичної інформації для її власника (сторона B): $sc \geq 10 \div 45$. З формули $P_T = P_t P_v$ очевидно, що за умов відсутності критичної інформації в ІС (тобто $q_{sc} = 0$) ймовірність $P_v = 0$. При $q_{sc} \gg sc$, тобто при значному рівні критичності ресурсу I й низьких витратах на створення і функціонування СЗІ, ймовірність $P_v \to 1$. Загалом значення ймовірності P_v при $q_{sc} = const$ зростає зі спадом рівня інвестицій в СЗІ.

Припустимо, що при нульових інвестуваннях у СЗІ організації $P_v = 1$ вихідний інформаційний ризик становить $R_1 = P_t q_{sc}$. Інвестування у СЗІ коштів у розмірі c призводить (за умов раціональних витрат цих коштів на потреби захисту) до того, що ймовірність успішного використання вразливості стає меншою за 1, тобто $P_v < 1$. Залишковий ризик в цьому випадку дорівнюватиме $R_1 = P_t P_v q_{sc}$, величина втрат, які вдалося попередити $R_1 - R_t = P_t q_{sc} - P_t P_v q_{sc} = (1 - P_v) P_t q_{sc}$, а відповідний «прибуток»

$$\Delta_R = R_I - R_t - c = (1 - P_v) P_t q_{sc} - c\,. \tag{9}$$

Замінюючи P_v в $R_1 - R_t = P_t q_{sc} - P_t P_v q_{sc} = (1 - P_v) P_t q_{sc}$ його розгорнутим виразом (8), отримуємо:

$$-c + \frac{sc}{q_{SC} + SC} P_t q_{sc} - 1 = 0 \tag{10}$$

З аналізу виразу (10) випливає, що якщо рівень інвестицій с перевищує деяке граничне значення $c_{max} = q_{sc}(P_t s - 1)/s$, «дохід» від введення захисту стає негативним, тобто в загальному випадку діапазон можливих значень с раціонально обмежити умовою: $0 < c < q_{sc}(P_t s - 1)/s$ – так званим діапазоном «розумних» інвестицій. З наведеної умови, виключаючи c, отримуємо нерівність: $0 < q_{sc}(P_t s - 1)/s$, вимога додержання якої накладає обмеження на можливі значення коефіцієнту s: $s > 1$.

Дослідженням співвідношення (9) на екстремум, вважаючи, що Δ_R є функцією змінної с, отримуємо вираз:

$$\frac{d\Delta_R}{dc} = \frac{s(q_{sc} + sc) - s^2 c}{(q_{sc} + sc)^2} P_t q_{sc} - 1 = 0, \tag{11}$$

який дозволяє визначити [12, 13] обсяг інвестицій c_{eff}, що забезпечує найбільше значення Δ_R (за термінологією Гордона-Лоеба c_{eff} – оптимальний розмір інвестицій):

$$c_{eff} = \frac{q_{SC}}{S}\sqrt{P_t s} - 1, \tag{12}$$

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

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_t s}}\,, R_t(c_{eff}) = P_v P_t q_{sc} = q_{sc}\sqrt{\frac{P_t}{S}}\,. \tag{13}$$

Аналіз формули (11) дає можливість оцінити максимальний обсяг інвестувань в СЗІ, який отримуємо з формули (11) при $P_t = 1$. Досліджуючи на екстремум залежність $c_{eff}(s) = \frac{q_{sc}}{s}(\sqrt{s} - 1)$, отримуємо:

$$\frac{dc_{eff}(s)}{ds} = q\left(s^{-2} - \frac{1}{2}s^{-\frac{3}{2}}\right) = 0, \tag{14}$$

що дає: $\max[c_{eff}(s)] = c_{eff}(4) = 0{,}25q$. Таким чином, максимальний обсяг інвестицій у СЗІ становить 25% від вартості q ресурсу, який є об'єктом захисту. Слід відмітити, що відповідно до практичного досвіду, накопиченого у сфері захисту інформації, значення $s \geq 10 \div 45$, причому для високоефективних рішень $s = 40 \div 60$, тобто рівень інвестувань може бути зменшений до 11-13 %.

Крім того зазначимо, що всі дані, необхідні для обчислення інвестицій в інформаційну безпеку організації (компанії, фірми), є її власними даними, які їй беззаперечно відомі і можуть бути застосовані для розрахунків, єдиним винятком є коефіцієнт s, пов'язаний з існуючою у світовій практиці залежністю між рівнем інвестицій c у захист та цінністю q_{sc} критичної інформації.

III Порівняння результатів оцінки інформаційних ризиків та визначення інвестицій у інформаційну безпеку при застосуванні економіко-вартісних моделей

Зважаючи на наявність суттєвих відмінностей між моделлю Гордона-Лоеба та економіко-вартісною моделлю, зокрема, розбіжності в отриманих оцінках максимального обсягу інвестицій у СЗІ, становить інтерес співставлення цих моделей у достатньо широкому діапазоні їх можливих застосувань. Наразі задля порівння результатів оцінки інформаційних ризиків та визначення обсягу інвестицій в інформаційну безпеку можна скористатися даними, які приводять Гордон та Лоеб в своїй статті 2015 року, наведеними в таблиці 1.

Таблиця 1 – Обсяги інвестицій в інформаційну безпеку за моделлю Гордона та Лоеба

Відсоток соціальної вартості, як співвідношення $100*L^e/L^p$	Приватні втрати при успішній реалізації загрози для приватних ресурсів L^p	Оптимальні інвестиції в інформаційну безпеку z*, на основі приватних втрат	Оптимальні інвестиції в інформаційну безпеку z*, на основі соціальних втрат (приватних і зовнішніх)	Відсоток недоінвестування в інформаційну безпеку за відсутності інформації про соц. втрати
0%	$400000	$60000	$60000	0%
20%	$400000	$60000	$75,271	20.29%
40%	$400000	$60000	$89,315	32.82%
60%	$400000	$60000	$102,386	41.40%
80%	$400000	$60000	$114,663	47.67%
100%	$400000	$60000	$126,274	52.48%
120%	$400000	$60000	$137,318	56.31%
140%	$400000	$60000	$147,871	59.42%
160%	$400000	$60000	$157,992	62.02%
180%	$400000	$60000	$167,731	64.23%
200%	$400000	$60000	$177,128	66.13%

Автори визначають оптимальні інвестиції в інформаційну безпеку на основі приватних втрат за формулою $z^*(v) = \left[(v\alpha\beta L^P)^{1/\beta+1} - 1\right]/\alpha$, а оптимальні інвестиції в інформаційну безпеку на основі соціальних втрат за формулою (6).

Для обчислення об'єму інвестицій та недоінвестувань пропонується використовувати функцію (6), яка, на погляд Гордона-Лоеба та враховуючи попередні дослідження, краще підходить для визначення оптимальних інвестицій в інформаційну безпеку, що однак викликає певні сумніви щодо її застосування, зокрема її можливостей адекватного відображення ситуації з інформаційними ризиками в компанії, для якої проводять аудит інформаційної безпеки. Крім того, нічим не аргументоване застосоване значення ймовірності порушення безпеки, яке дорівнює 0,64. Можна припустити, що автори приводять тестові дані або ж параметри, отримані за даними, які становлять державну або комерційну таємницею. Чому саме обрана ця функція, до кінця залишається не відомим.

Використавши дані, представлені в табл. 1, наводимо результати обрахунку інвестицій в інформаційну безпеку за допомогою економіко-вартісної моделі в табл. 2.

Таблиця 2 - Обсяги інвестицій в інформаційну безпеку за економіко-вартісною моделлю.

Відсоток соціальної вартості, як співвідношення $100*L^e/L^p$	Приватні втрати при успішній реалізації загрози для приватних ресурсів LP	Оптимальні інвестиції в інформаційну безпеку z* на основі приватних втрат	Оптимальні інвестиції в інформаційну безпеку z* на основі соціальних втрат (приватних і зовнішніх)	Відсоток недоінвестування в інформаційну безпеку за відсутності інформації про соц. втрати
0%	$400000	45090	45090	0,00%
20%	$400000	45090	54108	16,67%

40%	$400000	45090	63127	28,57%
60%	$400000	45090	72145	37,50%
80%	$400000	45090	81163	44,44%
100%	$400000	45090	90181	50,00%
120%	$400000	45090	99199	54,55%
140%	$400000	45090	108217	58,33%
160%	$400000	45090	117235	61,54%
180%	$400000	45090	126253	64,29%
200%	$400000	45090	135271	66,67%

Порівнявши між собою розрахункові результати, отримані за двома моделями на запропонованих даних, приходимо до висновку, що моделі дають невелику різницю в оцінці, але використовуючи економіко-вартісну модель, можна отримати більш точні значення об'єму інвестицій, які потрібні для покращення стану інформаційної безпеки компанії на 23–30%, скоротити процент недоінвестувань на 2–17% залежно від об'ємів сукупних втрат, яких зазнає компанія від реалізації загрози. Залежно від об'ємів ресурсів, що виділені компанією на заходи та засоби інформаційної безпеки, уточнення бюджету захисту на 20% може бути одним з рішень, що дозволить розвиватися іншим напрямкам діяльності компанії, а уточнення недоінвестувань на 5-10% дозволить реалізувати додаткові заходи та засоби захисту, які тільки покращать загальний стан захищеності.

IV Висновок

Проведено аналіз моделей, профільованих, серед іншого, для визначення оптимального обсягу інвестицій в систему захисту інформації. Не зважаючи на абсолютно різні підходи, на яких базуються ці моделі, вони дають доволі близькі результати, але мають ключові відмінності. Модель американських дослідників має формальний характер з явно вираженим наголосом на економіці, однак не враховує стану інформаційної безпеки на об'єкті захисту, реальних вразливостей системи захисту тощо. Економіко-вартісна модель ґрунтується на результатах аналізу реальних показників рівня захищеності інформаційної системи організації, потреб інформаційної безпеки, що вимагають використання реальних механізмів управління інформаційними ризиками, з урахуванням економічних тенденцій, а відтак дозволяє сподіватися на досягнення більш об'єктивних результатів при проведенні оцінки оптимального обсягу інвестицій в систему захисту інформації.

Традиційно актуальна проблема об'єктивного розподілу інвестицій на ринку захисту інформації в поєднанні із складнощами економічної ситуації вимагає раціонального розподілу загальних ресурсів, зокрема зменшення бюджетів, але досягнення кращих результатів захисту. Тому для спеціаліста у сфері захисту інформації змога об'єктивного зменшення обєму інвестицій на 20% та зменшення об'єму недоінвестувань на 10% має бути вагомим аргументом у виборі економіко-вартісної моделі як інструменту для оцінки ризиків та інвестицій у СЗІ.

Список використаної літератури: ***1.*** *Lukackij, A. V. Percentage of security - available at: http://www.it-world.ru/safety/58323.html.* ***2.*** *Gordon L. A. and Loeb M. P. The Economics of Information Security Investment // ACM Transaction on Information and System Security - 2002 - Vol. 5, №.4. - pp. 438-457.* ***3.*** *Архипов О. Є., Скиба А. В. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації // Захист інформації. – 2013. – Том15, №4. – С.366 – 375.* ***4.*** *Архипов А. Е., Архипова С. А., Скиба А. В. Применение затратно-стоимостных моделей для оценивания вероятностных параметров информационных рисков // Інформаційна безпека. – 2013. – №2(10). – С. 11-18.* ***5.*** *Скиба А. В., Хоріна О. І. Прогнозування соціально-психологічних та ситуаційних чинників активації злочинних думок і намірів у сфері інформаційної безпеки // Безпека інформації – 2015 - №21(2) – С. 165-173.* ***6.*** *Архипов О. Є., Скиба А. В., Хоріна О. І. Розширення економіко-вартісних моделей інформаційних ризиків за рахунок використання соціально-психологічних типів зловмисника. // Захист інформації – 2015 - № 1(17) - С. 60-72.* ***7.*** *Скиба А. В., Хоріна О. І. Прогнозування соціально-психологічних та ситуаційних чинників активації злочинних думок і намірів у сфері інформаційної безпеки.// Безпека інформації – 2015 - №21(2), С. 165-173.* ***8.*** *Gordon L., Loeb M., Lucyshyn W., Zhou L. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. // Journal of Information Security – 2015 - №6 – pp. 24-30.* ***9.*** *Willemson J. On the Gordon & Loeb Model for Information Security Investment // Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006), 2006. pp.101-112* ***10.*** *Willemson J. Extending the Gordon&Loeb Model for Information Security Investment // Fifth International Conference on Availability, Reliability, and Security (ARES 2010), 2010. pp 258-261.* ***11.*** *Архипов А. Е. Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков // Захист інформації – 2011. – №2 (51) – С. 69-76.*