УДК 005.52:005.334:004.056

АРХИПОВ Олександр Євгенійович
АРХИПОВА Євгенія Олександрівна

РИЗИКОВИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ГРАНИЧНОГО ОБСЯГУ ІНВЕСТИЦІЙ У ЗАХИСТ ІНФОРМАЦІЇ

Постановка проблеми. У сучасному суспільстві знань інформація є одним із основних ресурсів, потреба захисту якого усвідомлюється вже переважною більшістю суб'єктів господарювання. В цих умовах особливої актуальності набувають питання, пов'язані із захистом інформації, яка може представляти інтерес для потенційних конкурентів, інсайдерів, зловмисників тощо. З огляду на це виникає потреба виділення певного фінансування на розбудову та підтримку функціонування системи захисту інформації (СЗІ) в організаціях, установах та підприємствах різних форм власності. Враховуючи специфіку інформаційних ресурсів, зокрема складнощі, що виникають при спробі здійснення їх оцінювання зацікавленими сторонами, а також обмеженість фінансових ресурсів, особливо в період військово-політичної та економічної кризи, виникає потреба в адекватному оцінюванні рівня граничних інвестицій в СЗІ.

За даними О. Лукацького, бізнес-консультанта Cisco з безпеки, 78 % від обсягу всіх досліджуваних організацій 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]. Слід відзначити, що ці та подібні статистичні дані мають очевидний емпіричний характер та відображають поточну ситуацію з інвестуванням у сферу захисту інформації, яка стихійно склалася на момент зібрання цих даних. На жаль, подібні статистичні дані часто слугують основою для надання рекомендацій з оцінювання рівня інвестицій у побудову СЗІ в рамках так званого «практичного підходу» [2], тим самим створюючи ілюзію обґрунтованості насправді нічим не підкріплених рекомендацій, які можуть становити серйозну загрозу як через зумовлене ними недостатнє фінансування заходів із захисту інформації,так і у разі надлишковості інвестицій в побудову СЗІ, що призводить до невиправдано великих грошових втрат.

Аналіз останніх досліджень і публікацій. У 2002 році було опубліковано статтю американських дослідників в області економіки Лоуренса Гордона і Мартіна Лоеба «The Economics of Information Security Investment» [3], яка спричинила широкий суспільний резонанс, отримавши від науковців і практиків велику кількість відгуків й коментарів різного характеру, зокрема, схвальні та критичні зауваження, конструктивні пропозиції та доповнення [4; 5; 6].

В цій статті авторами було здійснено спробу теоретико-методологічного обґрунтування граничного обсягу інвестицій у безпеку інформації. Запропонований Гордоном і Лоебом підхід базується на використанні деякої функції ймовірності порушення захищеності інформаційних ресурсів (ФПЗІР), яка будується на системі з трьох аксіом, що формують певну сукупність вимог до властивостей ФПЗІР. Автори пропонують два класи залежностей, що задовольняють означеним вимогам, причому виконане ними подальше дослідження ФПЗІР для кожного з класів приводить до однакового висновку: оптимальний обсяг інвестицій у систему захисту інформації не може перевищувати 36,79 % від величини максимальних втрат, які можуть виникнути в разі реалізації загроз інформації. Тут слід наголосити, що в роботі Гордона і Лоеба відсутнє доведення повноти та достатності введеної системи аксіом, а тому не виключена можливість її доповнення, розвинення і, як наслідок, – модифікації отриманого висновку щодо величини можливих втрат. Саме тому цілком природною стала поява у 2006 році статті [4], де два класи функцій (залежностей), запропонованих Гордоном і Лоебом, доповнено ще чотирма, двох статей Дж. Вілмсона (J. Willemson) [5; 6], в яких дещо змінена та розширена вихідна система аксіом Гордона та Лоеба, інших модифікацій та доповнень підходу (моделі) Гордона-Лоеба. При цьому змінюється і відсоток оптимального обсягу інвестицій в СЗІ, зокрема в статті [5] він сягає 100 % від величини максимально можливих втрат, а в новій статті Гордона та Лоеба [8], де вони виступають у співавторстві із двома іншими дослідниками (William Lucyshyn, Lei Zhou), припускається, що оптимальний обсяг інвестицій може перевищувати 100 % від величини максимально можливих втрат.

Не вдаючись до детального аналізу позитивних та негативних властивостей підходу Гордона-Лоеба, акцентуємо увагу на одному суттєвому недоліку: у ньому використовується формально-апроксимативний спосіб побудови ФПЗІР, в якому не розглядається можливість врахування при формуванні структури й параметрів цієї функції відомостей про реальні

механізми розвитку та реалізації інформаційних загроз і ризиків. Це призводить до суттєвого обмеження практичних аспектів застосування зазначеного підходу та об'єктивності отриманих висновків, у тому числі й головного постулату авторів про величину оптимального обсягу інвестицій в захист інформації.

Метою статті є окреслення підходу до визначення оптимального обсягу інвестицій в систему захисту інформації, який враховує реальні механізми розвитку та реалізації інформаційних загроз і ризиків.

Виклад основного матеріалу. В цій ситуації видається корисним звернутися до моделі, запропонованій для дослідження економіко-мотиваційних відносин, характерних для ситуації «атака-захист» в інформаційній сфері [9; 10].

Розглянемо ситуацію, що виникає при реалізації атакуючою стороною A (зловмисник) загрози T стосовно деякого інформаційного ресурсу I, який належить стороні B. Вважатимемо, що D – загальна вартість витрат атакуючої сторони A на реалізацію загрози T, g – отриманий при цьому «виграш», величина якого обумовлюється цінністю ресурсу I для зловмисника. Збитки, яких зазнала в цій ситуації сторона B (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 щодо деякого інформаційного ресурсу I – це добуток

$$P_T = P_t P_v, \tag{1}$$

де P_t – ймовірність активації (виникнення) загрози стосовно інформаційного ресурсу I, P_v – ймовірність успішного використання зловмисником вразливостей інформаційної системи, яка містить ресурс I.

Значення ймовірності P_v залежить від рівня захищеності інформаційної системи, який у свою чергу обумовлюється обсягом інвестувань c в систему захисту інформації, що з певним наближенням враховується співвідношенням [9; 10]:

$$P_v = \frac{q}{q + sc}, \tag{2}$$

де s – коефіцієнт, яким визначає рівень ефективності інвестувань c в СЗІ.

Цей коефіцієнт має наступну властивість: чим більше значення s, тим нижче, за умови одного і того ж обсягу інвестицій у СЗІ, величина ймовірності успішної реалізації атак на інформаційну систему. Із наведеної формули випливає, що у разі відсутності цінної інформації в інформаційній системі (тобто $q = 0$) ймовірність $P_v = 0$. Коли вартість q ресурсу I висока або дуже висока, однак витрати на створення і функціонування СЗІ низькі, тобто $q >> sc$, 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 $0 < P_v < 1$. У загальному випадку значення ймовірності P_v при $q = const$ зростають зі спадом рівня інвестицій c в СЗІ і, навпаки, спадають зі зростанням їх обсягу.

Формули (1), (2) дозволяють побудувати оптимізаційну схему, за якою можна буде зробити висновки щодо ефективності та доцільності інвестицій у СЗІ організації. Для цього припустимо [10], що при нульових інвестуваннях у СЗІ організації $P_v = 1$ й вихідний інформаційний ризик становить $R_1 = P_t q$. Інвестування у СЗІ коштів у розмірі c призводить (за умов раціонального використання 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 $R_T = P_t P_v q$, 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» –

$$\Delta_R = R_1 - R_T - c = (1 - P_v) P_t q - c . \qquad (3)$$

Замінюючи P_v в формулі (3) його розгорнутим виразом (2), отримуємо:

$$-c + \frac{sc}{q + sc} P_t q = \Delta_R . \qquad (4)$$

Із аналізу виразу (4) випливає, що якщо рівень інвестицій c перевищує деяке граничне значення $c_{max} = q(P_t s - 1)/s$, «прибуток» від введення захисту стає негативним, тобто у загальному випадку діапазон можливих значень с раціонально обмежити умовою: $0 < c < q(s - 1)/s$ – так званим діапазоном «розумних» інвестицій. З наведеної умови, виключаючи c, отримуємо нерівність: $0 < q(s - 1)/s$, вимога додержання якої накладає обмеження на можливі значення коефіцієнту s: $s > 1$.

Досліджуючи співвідношення (4) на екстремум (вважаючи, що Δ_R є функцією змінної c), отримуємо вираз:

$$\frac{d\Delta_R}{dc} = \frac{s(q+sc) - s^2 c}{(q+sc)^2} P_t q - 1 = 0, \tag{5}$$

з умов виконання якого [10] визначаємо обсяг інвестицій c_{eff}, що забезпечує отримання найбільшого значення Δ_R (яке за термінологією Гордона-Лоеба називається оптимальним розміром інвестицій):

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

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

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

Аналіз формули (6) дає можливість оцінити максимальний обсяг інвестувань в СЗІ. Досліджуючи на екстремум залежність (6) як функцію змінної s, отримуємо:

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

Із рівності (8) знаходимо, що свого екстремуму функція $c_{eff}(s)$ досягає при значенні $s = 4/P_t$. Цьому значенню змінної s відповідає максимум функції $c_{eff}(s)$:

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

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. Необхідно підкреслити, що згідно із практичним досвідом,

накопиченим у сфері захисту інформації, значення $s \geq 10 \div 45$ [9; 10], причому для високоефективних рішень $s = 40 \div 60$. Тому у відповідності з формулою (6) навіть при $P_t = 1$ обсяг інвестицій в СЗІ може дорівнювати 11–13 % вартості ресурсу, що захищається.

Слід зазначити, що введене Гордоном та Лоебом поняття оптимального обсягу інвестицій в СЗІ є досить суперечливим, оскільки визначає оптимальним той рівень інвестицій $c_{eff\ \max}$, за якого максимізується різниця між величиною попереджених втрат $R_1 - R_T$ і обсягом с інвестицій в СЗІ, що забезпечили зниження ризику до значення R_T. При цьому абсолютно не враховуються такі важливі аспекти, як ступінь ефективності використання зроблених у СЗІ інвестицій або рівень підготовки та ресурсний потенціал атакуючої сторони. Врахувати ці аспекти можна було б шляхом введення додаткових показників захищеності ресурсу I, наприклад, отриманих вище ймовірності $P_v(c_{eff})$ і ризику $R_T(c_{eff})$, однак при цьому зникає одна з основних переваг підходу Гордона-Лоеба – мінімальний обсяг вихідної інформації, що залучається для оцінки максимального обсягу інвестицій в СЗІ. Розглянемо цей суперечливий момент більш детально.

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 виходячи з власного розуміння його цінності q у порівнянні з розумно достатніми (знову-таки з точки зору сторони В) витратами на захист. При цьому цінність ресурсу I, що залежить від важливості та значущості ресурсу для його власника В, зазвичай, збігається з величиною втрат у разі ураження (викрадення, модифікації тощо) цього ресурсу. Однак реальний ступінь захищеності ресурсу I значною мірою визначається інтенсивністю і силою атак сторони А, що залежать від її уявлень про цінність жаданого нею 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 буде оцінка, що розраховується за формулою:

$$P_v = \frac{g}{g + sc}. \qquad (10)$$

За однакового розуміння цінності інформації сторонами A і B$g=q$. Тоді оцінки, отримані із використанням формул (2), (10), збігаються, у зв'язку з чим справедливі всі наведені вище співвідношення і висновки. Але, зазвичай, уявлення сторін A і B про цінність інформації асиметричні. Тому виникає потреба вибору однієї з двох формул ((2) чи (10)): тієї, що базується на вартості ресурсу з точки зору зловмисника чи на оцінці вартості ресурсу з точки зору його власника.

Для власника ресурсу I (сторона B) його цінність q, зазвичай, розраховується на основі аналізу вартісних аспектів створення цього ресурсу, причому така процедура розрахунку часто носить типізований характер, а отримані оцінки достатньо стійкі.

Для атакуючої сторони A цінність g «добутої» інформації формується на основі ринкової вартості ресурсу I та кількості потенційних покупців, що бажають його придбати. Ще один ймовірний сценарій формування g: «добута» стороною A інформація являє собою інформацію з обмеженим доступом (ІзОД), поява якої у відкритому доступі може завдати шкоди ряду третіх сторін. Наслідком такої ситуації є пред'явлення цими сторонами претензій стороні B, яка не забезпечила збереження ІзОД, причому обсяг претензій у грошовому еквіваленті становитиме g [13]. Характерною особливістю оцінювання значення g є багатоваріантність розвитку ситуації у разі досягнення успіху атакуючою стороною A, погана прогнозованість кінцевих результатів, їх залежність від безлічі зовнішніх обставин та, як наслідок, нестабільність і нестійкість отримуваних оціночних значень g.

Припустимо, що $g \neq q$, причому стороні B, що захищається, відома оцінка вартості ресурсу з точки зору зловмисника. Тоді з урахуванням формули (10) отримуємо для співвідношення (4) нову форму подання:

$$-c + \frac{sc}{g + sc} P_t q = \Delta_R, \tag{11}$$

а кінцеві вирази (6), (9) набудуть вигляду:

$$c_{eff} = \frac{q}{s}\sqrt{P_t s} - \frac{g}{s}, \tag{12}$$

$$\max[c_{eff}(s)] = c_{eff}(4g^2 / P_t q^2) = 0{,}25 q^2 P_t / g\ . \tag{13}$$

Найбільшою величина оптимальних інвестицій в СЗІ виявляється при $P_t = 1$ і складає $c_{eff\ \max} = 0{,}25q^2 / g$. Аналіз останнього виразу, а також зіставлення вихідних формул (2), (6), (9), отриманих для випадку $g = q$, з відповідними їм співвідношеннями при $g \neq q$, показує, що розбіжність g і q може стати причиною недостатнього або, навпаки, – надлишкового інвестування в СЗІ. Зокрема, при $g>q$ розрахунки, проведені із припущенням, що $g = q$, призводять до заниження значення ймовірності P_v і недостатнього інвестування в СЗІ (всі показники занижені в g/q разів), при $g<q$ ситуація діаметрально протилежна. Для отримання об'єктивних даних про *найбільшу* величину оптимальних інвестицій в СЗІ у разі $g>q$ бажано користуватися формулою (10) і отримуваними на її основі співвідношеннями (11)–(13), тому окрім відомостей про рівень втрат q сторони B, що захищається, необхідна інформація про цінність ресурсу I для атакуючої сторони A. У разі $g \leq q$ для оцінювання *найбільшої* величини оптимальних інвестицій в СЗІ слід використовувати співвідношення (9), враховуючи при цьому зроблене вище зауваження про нестабільність і нестійкість отримуваних оціночних значень g. У зв'язку з цим цікавою є можливість застосування інших моделей, що описують альтернативні розглянутим імовірнісні параметри ризику.

Постановка і способи вирішення завдання 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 [2]. 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 коефіцієнта ефективності інвестицій s залежить не тільки від поведінки сторони, що захищається B, але і від зусиль та цілеспрямованості дій атакуючої сторони A. 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 [9; 10]:

$$P_t = \frac{g - D}{g} = 1 - \frac{D}{g}. \qquad (14)$$

Змістовний аспект отриманої формули пояснюється наступним чином: 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 зловмисника незначна, то економічні мотиви для виникнення загрози практично відсутні. Зокрема, якщо очікувані витрати D при реалізації атаки дорівнюють потенційному «виграшу» g, який принесе атакуючій стороні реалізація (використання) інформаційного ресурсу, зловмисник не отримає жодного прибутку, а при перевищенні очікуваних витрат D над потенційним «виграшем» g, який принесе атакуючій стороні інформаційний ресурс, зловмисник понесе збитки. Тобто в обох випадках атака стає нерентабельною, тому ймовірність активації загрози у цих випадках фактично дорівнює нулю.

Для ймовірності P_v врахування ресурсних можливостей атакуючої сторони A здійснюється шляхом множення значення інвестицій c в знаменнику формули (2) на мультиплікатор c/D, що дозволяє врахувати інвестиції D, які здійснюються стороною A в реалізацію атаки [11; 12]:

$$P_v(c, D) = \frac{q}{q + s\dfrac{c^2}{D}}. \tag{15}$$

Очевидно, що зростання витрат D обумовлює збільшення ймовірності P_v, тоді як збільшення інвестицій c у захист інформації дає протилежний ефект. Використання формул (14), (15) для обчислення ризику призводить до виразу виду:

$$R_T = P_t \frac{q}{q + s\dfrac{c^2}{D}} q = (1 - \frac{D}{g}) \frac{q^2 D}{qD + sc^2}. \tag{16}$$

На жаль, застосування знайденого ризику (16) для подальшої реалізації оптимізаційної процедури, аналогічної розглянутій вище (вирази (5), (6)), не дозволяє отримати рішення у явному вигляді. Залежність $R_1 - R_T = (1 - P_v) P_t q$ після підстановки в неї виразу (16) набуває логістичного

характеру, а аналіз нерівності $\Delta_R = R_1 - R_T - c \geq 0$ дає можливість лише визначити діапазон розумних інвестицій:

$$\frac{qP_t}{2}\left(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}\right) \leq c \leq \frac{qP_t}{2}\left(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}\right). \quad (17)$$

Потреба обчислення квадратного кореня у формулі (17) обумовлює очевидне обмеження $1 \geq 4D / sqP_t^2$, яке трансформується у нерівність виду:

$$D \leq 0{,}25sqP_t^2, \quad (18)$$

що накладається на обсяг інвестицій атакуючої сторони A. Крім того, необхідність застосування формули (14) для оцінювання ймовірності активації (виникнення) загрози T передбачає, що зловмисник очікує отримати від здобутої (викраденої) інформації більше, ніж він витратив на організацію її здобуття, тобто $g \geq D$. Дослідження співвідношення (16) за умови $D = 0$ дозволяє визначити, що максимальне значення розумних інвестицій в СЗІ не повинно перевищувати обсягу потенційних втрат q у разі викрадення ресурсу, який міститься в інформаційній системі, що захищається. Зі збільшенням значень D, при $D \to 0{,}25sqP_t^2$, права і ліва межі діапазону (17) 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 двох наведених вище обмежень $D \leq 0{,}25sgP_t^2$ і $g \geq D$ характерно для ситуації, коли атакуюча сторона A в своїх діях керується виключно принципом економічної доцільності (розумної достатності).

Однак, як показано в [11; 12], за певних обставин принцип економічної доцільності може не виконуватися. Це стосується ситуації, в якій атакуюча сторона для досягнення своїх цілей вдається до послуг найманого виконавця, який за будь-яких обставин повинен виконувати поставлене перед ним завдання (тобто для нього ймовірність активації загрози дорівнює одиниці й, відповідно, $P_T \equiv P_v$). Типовим прикладом подібної ситуації є виконання завдання співробітником спецслужби, що є професіоналом, підготовленим до здійснення атак в кіберпросторі. У разі важливості поставленої перед ним мети такий «зловмисник-виконавець» може розраховувати на широке залучення додаткових ресурсів: фінансових, технічних, інформаційно-аналі-

тичних, оперативних. На практиці це означає, що у разі залучення «зловмисника-виконавця» існує велика ймовірність реалізації ним високовитратних атак. Якщо ж можливі витрати зловмисника на отримання потрібного йому ресурсу практично нічим не обмежені, то ймовірність успішного виконання ним своєї задачі наближується до одиниці. У 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.

Висновки. Наведений підхід до визначення оптимального обсягу інвестицій в систему захисту інформації позбавлений недоліків, властивих підходу Гордона-Лоеба і його модифікаціям, які не дозволяють отримати однозначне рішення щодо оптимального обсягу таких інвестицій через суб'єктивний формально-апроксимативний спосіб побудови моделі захищеності інформаційних ресурсів.

Запропонований спосіб визначення оптимального обсягу інвестицій в систему захисту інформації ґрунтується на аналізі моделі інформаційних ризиків, структура і параметри якої базуються на використанні відомостей про реальні механізми розвитку та реалізації інформаційних загроз і ризиків, у тому числі на моделях мотиваційно-вартісних і економіко-фінансових відносин, характерних для ситуації «атака–захист» в інформаційній сфері. Максимальний обсяг оптимальних інвестицій в СЗІ за результатами аналізу представленої моделі інформаційних ризиків становить 25 % вартості інформаційного ресурсу, який є об'єктом захисту.

Список використаних джерел

1. Лукацкий А. В. Процент безопасности / А. В. Лукацкий [Электронный ресурс]. – 2013. – Режим доступа : http://www.it-world.ru/safety/58323.html.

2. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М. : Компания АйТи, ДМК Пресс, 2004. – 384 с.

3. Gordon L. A., Loeb M. P. The Economics of Information Security Investment // ACM Transaction on Information and System Security – 2002. – Vol. 5. – № 4. – pp. 438–457.

4. Hausken K. Returns to Information Security Investment: The Effect of Alternative Information Security BreachFunctions on Optimal Investment and Sensitivity toVulnerability // Information Systems Frontiers. – 2006. – № 5(8). – pp. 338–349.

5. Willemson J. On the Gordon & Loeb Model for InformationSecurity Investment // Proceedings of The FifthWorkshop on the

Economics of Information Security(WEIS 2006), 2006. pp.101-112

6. Архипов О. Є. Особливості визначення обсягу інвестицій в систему захисту інформаційних ресурсів / О. Є. Архипов, Є. О. Архипова // Інвестиції: практика та досвід. – 2015. – № 11. – С. 71–74.

7. Willemson J. Extending the Gordon & Loeb Model for Information Security Investment // Fifth International Conference on Availability, Reliability, and Security (ARES2010), 2010. Pp. 258–261.

8. Gordon, L. A., and Loeb, M. P. and Lucyshyn,W. and 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, vol. 6, pp. 24–30.

9. Архипов А. Е. Применение мотивационно-стоимостных моделей для описания вероятностных соотношений в системе «атака-защита»/ А. Е. Архипов, С. А. Архипова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2008. – Вип. 1(16). – С. 57–61.

10. Архипов А. Е. Применение экономико-мотивационных соотношений для оценивания вероятностных параметров информационных рисков / А. Е. Архипов // Захист інформації. – 2011. – № 2(51). – С. 69–76.

11. Архипов О. Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Є. Архипов, А. В. Скиба // Захист інформації. – 2013. – Т. 15, № 4. – С. 366–375.

12. Архипов А. Е. Применение затратно-стоимостных моделей для оценивания вероятностных параметров информационных рисков / А. Е. Архипов, С. А. Архипова, А. В. Скиба // Інформаційна безпека. – 2013. – № 2(10). – С. 11–18.

13. Архипов О. Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою : моногр. / О. Є. Архипов, О. Є. Муратов. – К. : Наук.-вид. відділ НА СБ України, 2011. – 195 с.

Аннотация: Изложен подход к определению оптимального объема инвестиций в систему защиты информации, который учитывает реальные механизмы развития и реализации информационных угроз и рисков.

Ключевые слова: информация, информационный ресурс, риск, инвестиции, система защиты информации.

Abstract: A way to determine the optimal volume of investment into the system of information security that takes into account the real mechanisms of the development and implementation of information security threats and risks is outlined.

Key words: information, information resource, risk, investment, system of information security.