УДК 005.52: 005.334: 004.056

О. Є. Архипов,
д. техн. н., професор кафедри інформаційної безпеки,
Національний технічний університет України "Київський політехнічний інститут", м. Київ
Є. О. Архипова,
к. філос. н., доцент кафедри теорії та практики управління,
Національний технічний університет України "Київський політехнічний інститут", м. Київ

ОСОБЛИВОСТІ ВИЗНАЧЕННЯ ОБСЯГУ ІНВЕСТИЦІЙ В СИСТЕМУ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

O. Arkhypov,
Doctor of Technical Sciences, Professor of the Information Security Department,
National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv
Ye. Arkhypova,
PhD in Philosophy, Associate Professor of the Department of Theory and Practice of Management,
National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv

FEATURES OF THE DEFINITION OF THE VOLUME OF INVESTMENT IN PROTECTION OF INFORMATION RESOURCES

Стаття присвячена проблемі визначення оптимального розміру інвестицій у систему захисту інформації. Наголошено на важливості інвестицій у захист інформаційних ресурсів на всіх рівнях системи державного управління. Здійснено аналіз публікацій, що містять матеріали, пов'язані із дослідженням та розвитком підходу Гордона-Лоеба, в якому обгрунтовується граничний обсяг інвестицій у безпеку інформації. Показано, що цей підхід не дає змоги отримати єдине доказово підтверджене рішення щодо оптимального обсягу інвестицій в систему захисту інформації через суб'єктивний формально-апроксимативний спосіб побудови моделі, на якій грунтується отримана оптимальна оцінка.

Запропонований підхід до дослідження задачі визначення оптимального обсягу інвестицій в систему захисту інформації заснований на аналізі моделі інформаційних ризиків, формування структури й параметрів якої базується на використанні відомостей про реальні механізми розвитку та реалізації інформаційних загроз і ризиків, зокрема на моделях мотиваційно-вартісних та економіко-фінансових відносин, характерних для ситуації "атака-захист" в інформаційній сфері.

За результатами аналізу моделі інформаційних ризиків отримано оцінку максимального обсягу оптимальних інвестицій у систему захисту інформації, яка становить 25 % від вартості інформаційного ресурсу, який є об'єктом захисту. Зазначено, що при застосуванні в системі захисту інформації високоефективних рішень рівень інвестувань може бути зменшений до 11—13 їх вартості.

The article devoted to a problem of determining the optimal size of the investment in information security system. Emphasized the importance of investment in the protection of information resources at all levels of public administration. The Exercised the analysis of publications which contained materials related to research and development approach of Gordon and Loeb, which justified limiting investment in information security. It is shown that this approach does not allow to receive only conclusively confirmed decision on optimal investment in information security through a subjective formal approximatively way of building the model of obtained optimum evaluation.

Proposed approach to the study of the problem of determining the optimal investment in information security based on an analysis of information risks model, determining the structure and parameters of which is based on the use of information about the real mechanisms of development and implementation of information security threats and risks, including the models motivational value and economic and financial relations specific to the situation of "attack-defense" in the information sector.

According to the analysis of information risk model received the assessment of maximum amount of optimal investment in information security system, which is come to 25% of the cost of information resource that is protected. It is noted that the application of highly efficient solutions in the system of information security the investuvan level may be reduced to 11—13 % of their value.

Ключові слова: захист інформації, рівень інвестицій, інформаційні ресурси, інформаційні загрози, ймовірність реалізації загрози, державне управління.

Key words: data protection, the level of investment, information resources, information threats, cost resource, probability of threat realization, public administration.

ПОСТАНОВКА ПРОБЛЕМИ

На поточний момент необхідність захисту інформації, в тому числі в державному управлінні, а відтак, необхідність інвестування коштів в її безпеку не викликає сумнівів. На тому, що інформація в сучасному світі є чи не одним з основних ресурсів розвитку людини та суспільства, акценту-

ють увагу багато вчених, які працюють як в царині гуманітарно-економічних наук (В. Горбулін, А. Давиденко, О. Додонов, В. Іноземцев, М. Кастельс, М. Кобрин, Й. Масуда, А. Пелещишин, Е. Тоффлер тощо), так і в галузі точних наук (А. Антонюк, О. Астахов, О. Додонов, О. Корченко, С. Расторгуєв, О. Щербаков та інші). Тим не менше питання співвідношення витрат на побудову системи захисту інформації та можливих втрат від реалізації інформаційних загроз у разі її відсутності або недостатньої надійності досі залишається малодослідженим. З огляду на це наразі дуже актуальним слід визнати питання про визначення обсягів інвестицій, які доцільно вкладати у захист інформації, що і є завданням даної статі.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

У системі державного управління від загальнодержавного до регіонального й місцевого рівнів циркулює величезна кількість інформації та даних, зокрема документи, які містять державну або службову таємницю, різноманітні бази персональних даних. Держава має забезпечувати належний рівень безпеки власних інформаційних ресурсів, адже несанкціонований витік, знищення або викрадення принаймні деякої частини даних, які на них зберігаються, може призвести до значних матеріальних (потенційних чи реальних) втрат, нанесення суттєвих моральних та іміджевих збитків або навіть людських втрат, як, наприклад, у випадку витоку інформації щодо державних шифрів, системи урядового зв'язку, оперативних планів переміщення військової техніки тощо. Велика кількість інформації персонального характеру, що накопичується, обробляється та зберігається в державних установах місцевого рівня та приватних організаціях, в яких досить часто відсутні навіть елементарні засоби захисту інформації, також може виступати об'єктом неправомірних дій зловмисників.

З огляду на це, інформаційні ресурси та інформаційно-телекомунікаційні системи всіх рівнів, які забезпечують функціонування системи державного управління, повинні мати належний рівень захисту від несанкціонованих дій з інформацією, що в них циркулює. В той же час витрати на побудову системи захисту інформації можуть перевищувати обсяг потенційних втрат у разі її витоку, що робить необхідним вироблення алгоритмів обчислення оптимального та граничного обсягу можливих інвестицій в захист державних інформаційних ресурсів.

За даними О.Лукацького, бізнес-консультанта Cisco з безпеки, 78% від обсягу усіх 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]. На жаль, переважна більшість рекомендацій щодо обсягу інвестицій формується з подібних до наведеної вище довідок, тобто носить емпіричний характер, базуючись виключно на узагальненні досвіду розробки та експлуатації існуючих систем захисту інформації. Саме це пояснює ту увагу, яку привернула до себе опублікована у 2002 р. стаття американських дослідників в області економіки Лоуренса Гордона і Мартіна Лоеба [2], в якій зроблено спробу теоретико-методологічного обгрунтування граничного обсягу інвестицій у безпеку інформації. Поява цієї статті викликала широкий резонанс в наукових та професійних колах, свідченням чого є численні відгуки та коментарі різного характеру, зокрема позитивні та критичні зауваження, конструктивні пропозиції та доповнення [3; 4].

Запропонована Гордоном і Лоебом модель (далі — модель Г-Л) — так звана функція ймовірності порушення захищеності інформаційних ресурсів (ФПЗІР) — базується на системі з трьох аксіом, що формують певну сукупність вимог до властивостей ФПЗІР. Автори пропонують два класи залежностей, які задовольняють означеним вимогам, причому виконане ними подальше дослідження ФПЗІР для кожного з класів приводить до однакового висновку: 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. Тут слід наголосити, що в роботі Гордона і Лоеба відсутнє доведення повноти та достатності введеної системи аксіом, не виключена можливість її доповнення, розвинення й, відповідно, модифікації отриманого висновку. Тому цілком природною стала поява у 2006 році статті [3], де два класи функцій (залежностей), запропонованих Гордоном і Лоебом, доповнено ще чотирма; статей Дж. Вілмсона (J.Willemson) [4; 5], в яких дещо змінена та розширена вихідна система аксіом Гордона і Лоеба; інших численних модернізацій та доповнень базової моделі Г-Л. При цьому змінюються і відсоток оптимального обсягу інвестицій в СЗІ, зокрема в статті [4] він сягає 100 % від величини максимально можливих втрат, а в новій статті Гордона та Лоеба [5], де вони виступають у співавторстві із двома іншими дослідниками (William Lucyshyn, Lei Zhou), припускається, що оптимальний обсяг інвестицій може і перевищувати 100 % від цієї величини.

Не вдаючись до детального аналізу позитивних та негативних властивостей моделі Г-Л, зазначимо, що як для самої моделі, так і для її численних модифікацій характерна суттєва вада: формально-апроксимативний спосіб побудови моделі, за яким практично повністю виключається можливість врахування при формуванні структури й параметрів моделі відомостей про реальні механізми розвитку та реалізації інформаційних загроз і ризиків. Це призводить до суттєвого обмеження практичних аспектів застосування означеної моделі та об'єктивності отриманих висновків, в тому числі і головного постулату про величину оптимального обсягу інвестицій в захист інформації.

У цій ситуації інтерес представляють моделі, запропоновані для дослідження мотиваційно-вартісних та економіко-фінансових відносин, характерних для ситуації "атака-захист" в інформаційній сфері [7, 8].

Розглянемо ситуацію, що виникає при реалізації атакуючою стороною *A* (зловмисник) загрози *T* відносно 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.

Наведені дані дають вартісну характеристику ситуації "атака-захист". На основі цих відомостей можна побудувати логіко-евристичну схему експертного оцінювання ймовірнісних характеристик, що використовуються для обчислення інформаційних ризиків.

Чистий прибуток зловмисника в разі успішної реалізації загрози *T* складає $Q = g - D$. Якщо цінність g ресурсу *I* для атакуючої сторони *A* значна, зокрема, якщо $g >> D$, 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 $g=D$) атака ресурсу *I* стає недоцільною, в цьому випадку $P_t = 0$. Для $g<D$ спроба реалізації

загрози *T* втрачає будь-який економічний сенс. Виходячи з цих міркувань, в [7] запропоновано співвідношення:

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

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

У загальному випадку ймовірність реалізації загрози *T* — це добуток

$$P_T = P_t P_v \quad (2),$$

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 с в систему захисту інформації (СЗІ), що з певним наближенням враховується співвідношенням [7; 8]:

$$P_v = \frac{q}{q + sc} \quad (3),$$

де *s* — коефіцієнт, яким визначається рівень ефективності інвестувань *c* в систему захисту інформації, а саме: чим більше значення *s*, тим нижче, за умови одного і того ж обсягу інвестицій с, величина ймовірності P_v. З формули (3) очевидно, що у разі відсутності критичної інформації в ІС (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* приділяє його захисту достатню увагу, значення *q* і *sc* співрозмірні, $P_v < 1$. Загалом значення ймовірності Pv при *q=const* зростають із спадом рівня інвестицій *c* в СЗІ і навпаки, збільшуються із зростанням їх обсягу.

Формули (1), (3) дозволяють побудувати оптимізаційну схему, за якою можна буде зробити висновки щодо ефективності та доцільності інвестицій у СЗІ організації. Для цього припустимо [8], 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 с 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 $R_t = P_t P_v q$, 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" —

$$\Delta_R = R_1 - R_t - c = (1 - P_v) P_t q - c \quad (4).$$

Замінюючи P_v в (4) його розгорнутим виразом (3), отримуємо:

$$-c + \frac{sc}{q + sc} P_t q = \Delta_R \quad (5),$$

З аналізу виразу (5) випливає, що якщо рівень інвестицій с перевищує деяке граничне значення $c_{max} = q(P_t s-1)/s$, "дохід" від введення захисту стає негативним, тобто в загальному випадку діапазон можливих значень с раціонально обмежити умовою: $0<c<q(P_t s-1)/s$ — так званим діапазоном "розумних" інвестицій. З наведеної умови, виключаючи *c*, отримуємо нерівність: $0<q(P_t s-1)/s$, вимога додержання якої накладає обмеження на можливі значення коефіцієнту *s*: $s > 1$.

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

$$\frac{d\Delta_R}{dc} = \frac{s(q + sc) - s^2 c}{(q + sc)^2} P_t q - 1 = 0 \quad (6),$$

який дозволяє визначити [8, 9] обсяг інвестицій c_{eff}, що забезпечує найбільше значення Δ_R (за термінологією Гордона-Лоеба c_{eff} — оптимальний розмір інвестицій):

$$c_{eff} = \frac{q}{s}(\sqrt{P_t s} - 1) \quad (7),$$

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

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_t s}}, \; R_t(c_{eff}) = P_v P_t q = q\sqrt{\frac{P_t}{s}} \quad (8).$$

Аналіз формули (7) дає можливість оцінити максимальний обсяг інвестувань в СЗІ, який отримуємо з формули (7) при $P_t = 1$. Досліджуючи на екстремум залежність $c_{eff}(s) = \frac{q}{s}(\sqrt{s} - 1)$, отримуємо:

$$\frac{dc_{eff}(s)}{ds} = q(s^{-2} - \frac{1}{2} s^{-3/2}) = 0 \quad (9),$$

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 зазначити, що відповідно до практичного досвіду, накопиченого у сфері захисту інформації, значення $s \geq 10 \div 45$ [7; 8], причому для високоефективних рішень $s \geq 40 \div 60$, тобто рівень інвестувань може бути зменшений до 11—13 %.

Вираз (3) — це оцінка ймовірності P_v так би мовити з середини, середовища ІС. Ця оцінка аж ніяк не враховує ресурсні можливості нападу. Щоб, наприклад, врахувати існуючий взаємозв'язок між витратами D на реалізацію загроз та рівнем інвестицій с у захист, запишемо (3) у вигляді [9; 10]:

$$P_v(c, D) = \frac{q}{q + s\frac{c^2}{D}} \quad (10).$$

Очевидно, що зростання витрат D обумовлює збільшення ймовірності P_v. Залежність $R_1 - R = (1 - P_v) P_t q$ в цьому випадку матиме логістичний характер, а діапазон "розумних" інвестицій визначатиметься співвідношенням:

$$\frac{qP_t}{2}(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}) < c < \frac{qP_t}{2}(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}) \quad (11),$$

коректним при дотриманні обмеження $D \leq sqP_t^2/4$. Як це витікає із співвідношення (11), для $D = 0$, тобто за умови відсутності інвестицій в атаку, "розумній" обсяг інве-

стицій с перебуває в інтервалі $0 < c < qP_t$ й, очевидно, $c \leq q$ цілковито залежить від ймовірності P_t активації (виникнення) загрози T.

Умова (11) отримана для випадку, коли існує ймовірність $P_v \leq 1$, тобто є дійсним обмеження $g > D$. Зовсім інша ситуація виникає у разі, коли інформаційну загрозу реалізує найнятий для цього виконавець (в загальному випадку це може бути спеціально створена група професіоналів, для яких це звичайна робота). В цьому випадку $P_t = 1$, атакуюча сторона просто виконує поставлене перед нею завдання і, залежно від його важливості, може розраховувати на залучення для підтримки своїх дій певних додаткових ресурсів: фінансових, технічних, інформаційно-аналітичних, оперативних, тобто існує велика ймовірність застосування для реалізації загроз високозатратних атак. Зокрема, як це випливає з виразу (10), якщо $D \to \infty$, то $P_v \to 1$, тобто можна очікувати появу дуже високих значень $P_{v\,max}$. На практиці це означає, що гарантовано захистити свою інформацію сторона B буде неспроможна.

ВИСНОВКИ

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

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

Література:

1. Лукацкий А. В. Процент безопасности [Електронний ресурс]. — 2013. — Режим доступу: http://www.it-world.ru/safety/58323.html

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

3. Hausken K. Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability // Information Systems Frontiers. — 2006. — No. 5 (8). — P. 338—349.

4. 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 .— P.101—112.

5. Willemson J. Extending the Gordon&Loeb Model for Information Security Investment // Fifth International Conference on Availability, Reliability, and Security (ARES 2010), 2010. — P. 258—261.

6. 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. — P. 24—30.

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

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

9. 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.

10. 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.

References:

1. Lukackij, A. V. (2014), "Percentage of security" available at: http://www.it-world.ru/safety/58323.html (Accessed 10.08.2014).

2. Gordon, L.A. and Loeb, M.P. (2002), "The Economics of Information Security Investment", ACM Transaction on Information and System Security, vol. 5, no. 4. pp. 438—457.

3. Hausken, K. (2006), "Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability", Information Systems Frontiers, vol. 5(8), pp. 338—349.

4. Willemson, J. (2006), "On the Gordon & Loeb Model for Information Security Investment", The Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge, UK, pp. 101—112.

5. Willemson, J. (2010), "Extending the Gordon&Loeb Model for Information Security Investment", Fifth International Conference on Availability, Reliability, and Security (ARES 2010), Krakov, pp 258—261.

6. Gordon, L.A. and Loeb, M.P. and Lucyshyn, W. and Zhou, L. (2015), "Externalities and the Magnitude of Cybersecurity Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model", Journal of Information Security, vol. 6, pp. 24—30.

7. Arhipov, A.E. and Arhipova, S.A. (2008), "Application of motivational-cost models to describe the probabilistic relationships in the attack-defense system", Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini, vol. 1 (16), pp. 57—61.

8. Arhipov, A.E. (2011), "Application of economic and motivational relations for estimating the probability parameters of information risks", Zakhyst informatsii, vol. 2 (51), pp. 69—76.

9. Arkhypov, O.Ye. and Skyba, A.V. (2013), "Information risks: methods and techniques of research, risk models and methods for their identification", Zakhyst informatsii, vol. 15 (4), pp. 366—375.

10. Arkhypov, O.Ye. and Arhipova, S.A. and Skyba, A.V. (2013), "Use of cost-cost models to estimate the probability parameters of information risks", Information security, vol. 2 (10), pp. 1—18.

Стаття надійшла до редакції 27.05.2015 р.