Корченко Александр Григорьевич, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой безопасности информационных технологий Национального авиационного университета.
E-mail: icaocentre@nau.edu.ua

Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедрою безпеки інформаційних технологій Національного авіаційного університету.

Korchenko Oleksandr, doctor of technical sciences, professor, laureate of the State Prize of Ukraine in Science and Technology, Head of Academic Department of IT-Security National Aviation University (Kyiv, Ukraine).

Казмирчук Светлана Владимировна, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: sv902@mail.ru

Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Kazmirchuk Svitlana, PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Гололобов Андрей Юрьевич, аспирант кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: burn2dust@gmail.com

Гололобов Андрій Юрійович, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.

Gololobov Andrew, postgraduate student of Academic Department of IT-Security National Aviation University (Kyiv, Ukraine).

УДК 004.056

ІНФОРМАЦІЙНІ РИЗИКИ: МЕТОДИ ТА СПОСОБИ ДОСЛІДЖЕННЯ, МОДЕЛІ РИЗИКІВ І МЕТОДИ ЇХ ІДЕНТИФІКАЦІЇ

Олександр Архипов, Андрій Скиба

Розглядаються нормативно-правові документи в області інформаційної безпеки, методи оцінювання інформаційних ризиків, зокрема економіко-вартісні моделі для ідентифікації ймовірнісних параметрів та структури інформаційних ризиків, застосування цих моделей для аналізу інвестицій в інформаційну безпеку. Звичайно для проведення адекватного оцінювання інформаційних ризиків та оптимізації обсягів інвестицій в інформаційну безпеку застосовуються підходи та процедури, що спираються на існуючі міжнародні стандарти з менеджменту ризиків інформаційної безпеки. Нажаль, ці стандарти мають переважно концептуально-рекомендаційний характер і не враховують багатьох факторів, котрі суттєво впливають на точність та об'єктивність оцінювання ризиків. Економіко-вартісний підхід до аналізу ризиків, зокрема відома модель Гордона-Лоеба, орієнтована переважно на дослідження оптимізаційних аспектів управління ризиками, проте практично виключає можливість врахування у цих дослідженнях конкретики реального об'єкту ризику. Запропоновано моделі, які використовують евристичні мотиваційно-вартісні механізми визначення параметрів та структури ризиків. Дані моделі дозволяють об'єднати викладені в міжнародних стандартах методи аналізу та оцінювання ризиків з можливостями оптимізаційних досліджень ризику, закладених в моделі Гордона-Лоеба. Задля забезпечення більшої адекватності цих моделей вимогам практичного застосування до їх структури передбачено введення інформації про психо-соціальні характеристики зловмисника.

Ключові слова: *Інформаційна безпека, стандарти з менеджменту ризиків інформаційної безпеки, методи оцінювання ризиків, дослідження інвестицій в інформаційну безпеку, психотипи зловмисників.*

Вступ. Швидкий розвиток інформаційних технологій обумовлює необхідність приділяти належну увагу забезпеченню інформаційної безпеки, відповідності її стану швидким змінам в технологіях, що забезпечує зменшення ймовірності настання ризиків, пов'язаних з інформаційними загрозами. Найбільшу увагу при формуванні систем інформаційної безпеки в вітчизняних компаніях, підприємствах, установах приділяють, як правило, виконанню вимог нормативно-методичної бази в сфері захисту інформації, визначаючи ці

вимоги як першооснову становлення системи інформаційної безпеки, що, однак, само по собі ще не створює гарантій достатнього рівня захисту. Організація може виділяти значні ресурси для забезпечення стійкості і стабільності функціонування корпоративних інформаційних систем, що однак не гарантує досягнення навіть мінімального рівня безпеки інформації. Суть проблеми полягає в тому, що при проектуванні та побудові системи захисту інформації основна увага має бути приділена не мінімізації впливів з певного переліку типових загроз, складеному відповідно до деякого уявного середовища функціонування організації, а виявленню та мінімізації інформаційних ризиків, пов'язаних з практичною діяльністю конкретної організації. Саме формування реального профілю ризиків, пов'язаних з процесами діяльності організації, зменшення цих ризиків або їх нейтралізація при збереженні постійного контролю ризикової ситуації становить суть провідних сучасних концепцій створення систем захисту інформації. На жаль, сама сутність методології ризиків обумовлює певні труднощі у своєму практичному застосуванні, бо вимагає обчислення високоточних оцінок інформаційних ризиків, оперування з ними й передбачає необхідність певної індивідуалізації, винятковості отриманих в рамках цього підходу рішень.

Для того, щоб отримати більш-менш чітке уявлення про ситуацію, пов'язану з можливостями практичного застосування методології ризиків в сфері інформаційної безпеки, розглянемо численні рекомендації та приклади застосування цієї методології, описані у міжнародних стандартах, національних нормативних документах та настановах з інформаційної безпеки.

Система стандартів у сфері оцінювання інформаційних ризиків. Проблема оцінювання та дослідження інформаційних ризиків звичайно асоціюється з британським стандартом BS 7799, насамперед з його двома частинами: першою – BS 7799-1 «Звід правил з менеджменту безпеки інформації» та другою – BS 7799-2 «Системи менеджменту безпекою інформації», в яких вперше питання аналізу стану безпеки інформації та формування її захисту були напряму пов'язані з інформаційними ризиками. Однак безпосередньо аспекти оцінювання та управління ризиками, гармонізовані із змістом двох перших частин, було докладно розглянуто у третій частині стандарту BS 7799-3 «Настанови з менеджменту ризиками безпеки інформації» [15]. Проте першим міжнародним стандартом з менеджменту ризиками став стандарт ISO/IEC TR 13335-3 «Настанови з менеджменту безпеки інформаційних технологій»(1998 р.), який, як і інші стандарти серії ISO/IEC 13335, є національним стандартом України. Через десять років, у 2008 р. було видано стандарт ISO/IEC 27005 «Менеджмент ризиками безпеки інформації» [20], який наразі став одним з провідних нормативних документів у сфері управління інформаційними ризиками.

Практично всі сучасні стандарти в області безпеки відображають спільний підхід до організації управління ризиками, що склався у міжнародній практиці. При цьому управління ризиками представляться як базова частина системи менеджменту якості організації. Стандарти носять відверто концептуальний характер, що дає змогу експертам з інформаційної безпеки реалізовувати будь-які методи, засоби та технології оцінювання, обробки та управління ризиками.

Вважається, що міжнародні стандарти, створені на основі аналізу та узагальнення найкращих методів, апробованих, як великими групами професіоналів так і провідними організаціями на практиці, в більшості випадків визначають найкращі варіанти дій при виникненні інцидентів в інформаційній безпеці. Використання стандартів збільшує цінність створюваної інформаційної системи або технології, але немає таких стандартів, які б охопили всі аспекти управління, безпеки та якості.

Еволюцію розвитку стандартів у сфері менеджменту ризиками безпеки інформації можна представити наступною схемою, зображеною на Рис.1.

Очевидно, що зміст еволюції – вихід нового стандарту на вищий якісний рівень через «сприйняття досвіду» від стандартів-попередників та узагальнення наслідків застосування стандартів із суміжних галузей. Відбувається позитивний процес заміщення старої серії стандартів IT безпеки ISO/IEC TR 13335, новою серією стандартів у сфері управління інформаційною безпекою - ISO/IEC 27000. Новий стандарт ISO/IEC 27005 замінив відразу два морально застарілих стандарти ISO/IEC TR 13335-3 [21] і ISO/IEC TR 13335-4 [22], які, однак, залишилися в числі базових документів для нового стандарту. Крім того, стандарт ISO/IEC 27005 також спирається на нормативно-методичні документи, наведені в його бібліографічному переліку: ISO/IEC 16085 [18], BS 31100[14], AS/NZS 4360[13] і NIST SP 800-30[24].

Суттєвий вплив на зміст нового стандарту виявила і розробка стандарту ISO/IEC 31000 «Ризик-менеджмент. Принципи та настанови», що тривала практично одночасно з розробкою

ISO/IEC 2705. Стандарт ISO/IEC 31000 узагальнив у собі найкращі тенденції світової практики по управлінні ризиками. В бібліографічному переліку цього стандарту такі стандарти, як: ISO/IEC 9001 – загальні вимоги до систем менеджменту якості, ISO/IEC 9004 – рекомендації для стійкого досягнення цілей в системах управління якістю, BS31100 – набір практичних і конкретних рекомендацій для менеджера інформаційної безпеки, ISO/IEC Guide 73 – набір термінів для управління ризиками, вже згаданий вище AS / NZS 4360 – загальні вимоги до умови управління ризиками. Уся нормативна документація, на якій базується стандарт ISO/IEC 31000, відноситься до галузі управління та контролю якістю і застосовна до різних сфер діяльності, включаючи і сферу інформаційної безпеки.

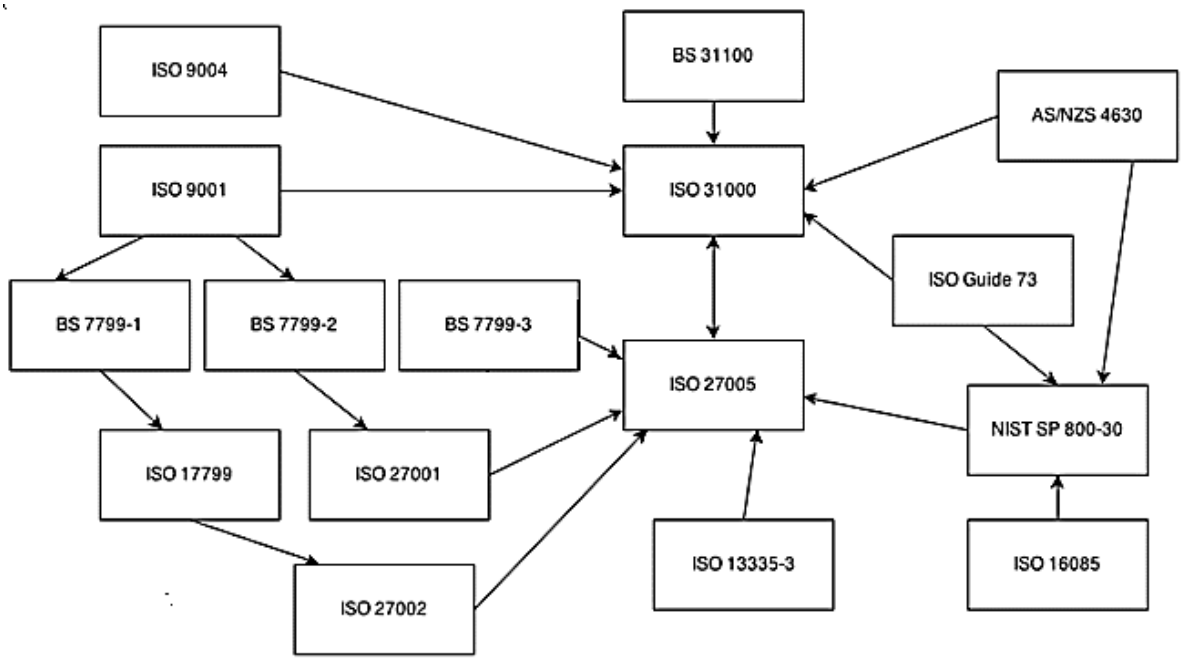

Рис.1. Еволюція стандартів менеджменту ризиками безпеки інформації

Тобто узагальнення найкращого міжгалузевого досвіду є ще однією перевагою стандарту ISO/IEC 27005, для якого ситуація виглядає наступною: з однієї сторони сильна теоретична база з практикою по управлінні безпекою, а з іншої – найкраще з досвіду управління та контролю якості, перевірене в багатьох сферах застосування.

Слід відзначити, що всупереч поширеним очікуванням, новий стандарт ISO/IEC 27005 зовсім не є міжнародною версією BS 7799-3[15]. Більш того, в ньому навіть не зустрічається згадки про останній стандарт. Структура та зміст цих стандартів істотно розрізняються, істотно різняться і джерела розробки. Незмінним залишається лише загальний понятійний апарат, загальний підхід до процесу управління ризиками.

Загалом можна зробити висновок про те, що для стандарту ISO/IEC 27005, на відміну від попередніх стандартів серії ISO/IEC 27000, в розробці яких використовувалися виключно напрацювання BSI та інших британських організацій, був врахований повною мірою існуючий міжнародний досвід.

Методики та рекомендації наведених вище стандартів базуються на двох основних підходах до представлення оцінок інформаційних ризиків [9,11]: якісному та кількісному.

Завданням якісної оцінки є визначення можливих видів ризиків, оцінка принципового рівня серйозності загроз, а також виділення чинників, які впливають на рівень обґрунтування різних можливих контрзаходів. Ці методики не надають кількісні або грошові значення компонентам і втратам. Вони достатньо популярні, відносно прості і розроблені, як правило, на основі вимог міжнародного стандарту ISO/IEC 17799:2005[19].

Кількісні методики надають реальні й осмислені чисельні значення всім елементам процесу аналізу ризиків. Цими елементами можуть бути вартість захисних заходів, цінність активу, збиток для бізнесу, частота виникнення загрози, ефективність захисних заходів, вірогідність використання уразливості і так далі. Кількісний аналіз дозволяє набути конкретного значення ймовірності (у відсотках) реалізації загрози. Кожен елемент у процесі аналізу вводиться в кількісному вигляді в рівняння для визначення загального й залишкового ризику.

Також доволі часто використовується комбінація цих двох підходів, як правило, на початкових

етапах аналізу інформаційних ризиків використовується якісний, а на кінцевому – саме отримання оцінки – кількісний.

Зважаючи на те, що оцінка ризиків на якісному рівні не дозволяє однозначно порівняти витрати на забезпечення інформаційної безпеки і отриманої від них віддачі (у вигляді зниження сумарного ризику), зосередимося на більш точному кількісному підході. Зазначимо, що в цьому разі процедура побудови систем захисту інформації (СЗІ) на базі методології інформаційних ризиків із застосування настанов основних стандартів характеризується низкою «вузьких» місць.

По-перше, це необхідність параметризації ризиків. Загальновживане математичне співвідношення, за яким обчислюються ризик, обумовлений можливою реалізацією загрози T, має вигляд:

$$r_T = P_T q = P_t P_V q, \qquad (1)$$

де P_T – ймовірність реалізації загрози T, q – збитки, що виникають за умов реалізації загрози T, P_t – ймовірність виникнення (активації) загрози T, P_V – ймовірність вдалого використання зловмисником уразливостей інформаційної системи, що призводить до реалізації загрози T. Тобто обчислення ризику потребує знання двох(P_T, q) або трьох (P_t, P_V, q)параметрів ризику r_T, які звичайно визначаються експертним шляхом [10,11,12], що може вельми суттєво погіршити якість оцінок ризиків, а відтак – абсолютно непрогнозовано вплинути на кінцеві результати менеджменту ризиків.

По-друге, наявність кількох загроз (уразливостей) характеризується відповідними частковими ризиками, сукупний вплив яких описується певним інтегральним ризиком, визначення якого в загальному випадку може бути досить складним [2].

По-третє, методики управління ризиками, розроблені за настановами стандартів, частіше за все спираються на перебірній підхід: розглядається кілька можливих варіантів побудови СЗІ, в яких рівні ризиків (інтегрального ризику) зменшуються до прийнятних значень, і далі за рішенням експерта визначається робочий варіант (можливо, він вибирається як найменш вартісний). При цьому питання якості робочого варіанту СЗІ (оптимальності прийнятого рішення про вибір цього варіанту СЗІ), ефективності інновацій в організацію СЗІ практично не досліджуються. Заміна експерта будь-яким інструментально-програмним засобом (ІПЗ) принципово ситуації не змінює, бо прототипом при розробці цих ІПЗ виступає саме експерт, тому практично всі найбільш поширені ІПЗ – це інтелектуалізовані інформаційні системи (системи підтримки прийняття рішень, експертні системи тощо), в яких реалізовані ти чи інші методи відображення та обробки знань.

Певною альтернативою управління ризиками на базі методик, представлених в стандартах, є застосування у менеджменті ризиків математичних моделей, що пов'язують рівень ризиків (збитків), обумовлених реалізацією інформаційних загроз, із обсягом інвестувань z в СЗІ [6,7,16,23,25]. Застосування цих моделей для аналізу та дослідження ризиків має на меті серед іншого забезпечити можливість оцінювання ефективності інвестувань у СЗІ та прогнозування характеристик ризиків залежно від рівня інвестицій в систему захисту.

Модельні дослідження інвестувань у системи захисту інформації. На сьогодні однією з найбільш поширених та відомих моделей, що застосовуються для аналізу ефективності інвестувань у СЗІ, є модель, розроблена двома американськими дослідниками в області економіки Лоуренсом Гордоном і Мартіном Лоебом з університету Мерілеңд у 2002 році [23]. Модель призначена для визначення економічно обґрунтованого інвестування в інформаційну безпеку.

В моделі Гордона-Лоеба розглядається одноперіодична економічна модель: фірма роздумує над тим скільки інвестувати в інформаційну безпеку. Зазвичай безпека інформації характеризується наступними показниками: L - потенційні збитки від витоку інформації, $S(z, v)$ – функція вразливості інформації, яка визначає ймовірність того, що інформацію буде викрадено, (тобто $S(z, v)$ – це функція ймовірності порушення безпеки), z – обсяг інвестицій у захист, v – вразливість інформації, яка визначається як ймовірність того, що атака буде успішною.

Пропонується розглянути деякі властивості функції $S(z, v)$. По-перше, автори пропонують вважати функцію $S(z, v)$ гладкою. Це зроблено для того, щоб мати можливість застосувати математичний апарат теорії оптимізації, для отримання необхідного економічного ефекту. Далі, апелюючи до природи інформаційних ризиків, автори роблять три достатньо слушних припущення відносно властивостей функції $S(z, v)$:

1. $S(z, v) = 0$ для будь-яких z.

Тобто якщо інформація абсолютно невразлива, вона залишається такою для будь-якого рівня інвестицій.

2. Для будь-яких v маємо: $S(0,v) = v$.

Тобто, якщо немає інвестувань в інформаційну безпеку, то функція ймовірності вразливості

інформації буде дорівнювати ймовірності цієї вразливості.

3. Для будь-яких $v \in (0,1)$ та будь-яких z, справедливо:

$$\partial \frac{d(z,v)}{dz} < 0, \text{ а } \partial^2 \frac{S(z,v)}{\partial z^2} > 0.$$

Тобто, якщо інвестування в інформаційну безпеку зростають, інформація стає більш захищеною, але темпи росту рівня захищеності менші за швидкість зростання інвестувань. Більш того, автори припускають, що для всіх $v \in (0,1)$ $\lim_{x \to \infty} S(z,v) \to 0$, тобто суттєве інвестування в безпеку призводить до зменшення ймовірності вразливості інформації майже до 0.

Проаналізувавши третє припущення, розуміємо, що навіть незначні інвестиції в інформаційну безпеку знижують ризики витоку інформації.

Дані припущення автори перевірили на великих об'ємах даних, практика показала, що ця модель придатна для застосовування в реальних умовах. Також для цієї моделі зроблені розширення [25] та вона пройшла практичну перевірку на емпіричних даних, отриманих за результатами дослідження японських підприємств [17], дані про які було надано державною інспекцією, що свідчить про їх високий коефіцієнт достовірності.

Автори приводять наступні формули для того щоб визначити кількість інвестувань в інформаційну безпеку, зазвичай нейтральна до ризику фірма порівняє очікуваний бонус від інвестування з вартістю інвестування. Очікуваний бонус від інвестицій у інформаційну безпеку (EBIS) визначається як зниження потенційних втрат завдяки додатковим витратам на безпеку:

$$EBIS(z) = \left[v - S(z,v) \right] L. \qquad (2)$$

Очікуваний бонус від інвестувань в інформаційну безпеку пояснюється, як непрямий прибуток в результаті інвестування в інформаційну безпеку, також це є ще одним напрямком дослідження. Даний напрямок ще не досліджувався, тому достовірно описати переваги від отриманого бонусу в результаті інвестицій в інформаційну безпеку не можна, також це потребує перевірки на реальних даних.

EBIS(z) записана як функція від z тому, що це єдина змінна, на яку може впливати фірма (v та L – це постійні параметри інформації). Очікуваний чистий дохід від інвестування в безпеку (*ENBIS*(z)):

$$ENBIS(z) = \left[v - S(s,v) \right] L - z. \qquad (3)$$

За термінологією ризиків *EBIS*(z) – це кількісна оцінка зменшення вихідного (початкового) ризику vL внаслідок освоєння інвестувань в систему захисту, *ENBIS*(z) – певна критеріальна ознака, яка містить в собі результат співставлення оцінки зменшення ризику з обсягом інвестицій z, що зумовили це зменшення. Таким чином, співвідношення (2), (3) містять відомості про економічну доцільність інвестувань в безпеку, необхідні для здійснення цілеспрямованого керування процесом менеджменту ризиків. Однак практичне застосування співвідношень (2), (3) (зокрема оцінювання кількісних значень *EBIS*(z), *ENBIS*(z)) потребує визначення структури та параметрів функції вразливості $S(z,v)$. В своїй роботі [23] Гордоном та Лоебом запропоновано для використання у якості функції вразливості $S(z,v)$двох широких класів функцій, дослідження та розвинення яких спричинило появу низки наукових публікацій, включаючи і статті вітчизняних авторів [7, 8]. На жаль, проблема вибору функції $S(z,v)$ дотепер вирішується у виключно суб'єктивний спосіб, а в численних публікаціях висвітлюються в основному описові та апроксимативні властивості варіантів цієї функції.

В зв'язку з цим після моделі Гордона-Лоеба доречно розглянути економіко-вартісні моделі, запропоновані в [3-6] для кількісного оцінювання параметрів інформаційних ризиків.

Для визначення ймовірнісних параметрів ризику в цих моделях використовуються певні характеристики мотиваційно-вартісних та економіко-фінансових відносин, характерних для ситуації «атака-захист» в інформаційній сфері. Розглянемо ситуацію, що виникає при реалізації атакуючою стороною А (зловмисник) загрози *T* відносно деякого інформаційного ресурсу *I*, який належить стороні В. Вважатимемо, що *D* – загальна вартість витрат атакуючої сторони А на реалізацію загрози *T*, *g* – отриманий при цьому «виграш», величина якого обумовлюється цінністю ресурсу *I* для зловмисника. Збитки, яких зазнала в цій ситуації сторона В (власник ресурсу *I*), тобто вартість критичної інформації с точки зору її власника, оцінюється ним як *q*, а загальна вартість реалізованого в ІС 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.

Застосування економіко-вартісних моделей для оцінювання ризиків та дослідження ефективності інвестицій в інформаційну безпеку. Чистий прибуток зловмисника в разі успішної реалізації загрози T складає:

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

Якщо цінність ресурсу I для атакуючої сторони А значна, інтенсивність потоку спроб доступу зловмисника до ресурсу I буде дуже високою. Зокрема, якщо $g>>D$, можна припустити, що ймовірність P_t активації (виникнення) загрози T буде практично дорівнювати 1, тобто 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 [3] для оцінювання значень ймовірності активації (виникнення) загрози T запропоновано співвідношення:

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

Однак в виразі (4) ніяк не враховується рівень індивідуальних мотиваційних характеристик зловмисника. Тому більш гнучким є варіант оцінювання ймовірності P_t за формулою [4,5]:

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

де введено коефіцієнт мотивації γ, що відображає ступінь впливу величини «виграшу» g на дії сторони А з активації загрози T.

Залежно від індивідуальних властивостей зловмисника коефіцієнт мотивації γ може бути як більше 1 (атакуючій стороні А властивий азарт, авантюризм, впевненість у своєму успіху), так і менший за 1 (зловмисник обережний, не гарячкує, воліє «мати синицю в руці, ніж журавля в небі»). Враховуючи, що значення ймовірності обмежуються діапазоном [0; 1], на область існування значень коефіцієнта мотивації γ накладається умова: $\gamma \geq (D/g)$.

Особливістю наведених вище результатів є те, що вони отримані для гіпотетичного зловмисника, який діє за принципом виключно економічної доцільності. Це типовий «зловмисник-прагматик». Однак можливі і інші варіанти мотивації виникнення загрози T, наприклад, ображений або мстивий зловмисник («зловмисник-месник»), домінантою дій якого є максимізація втрат q власника інформації за умов мінімальних особистих витрат D. Частіше за все причиною дій цього зловмисника є певні особисті мотиви, обумовлені непорозуміннями або конфліктними ситуаціями, що виникли за місцем роботи, служби, інше. Формула (6) в цьому випадку приймає вигляд:

$$P_t = \frac{\gamma q - D}{\gamma q} = 1 - \frac{D}{\gamma q}. \quad (7)$$

Слід зазначити, що наведені вище формули (6), (7) фактично віддзеркалюють певні сценарії дій зловмисника, що визначаються його психотипом, причому рівень домінантної психологічної риси зловмисника, яка є причиною його асоціальної поведінки, оцінюється саме коефіцієнтом γ. Очевидно можливо виділити декілька класів психотипів зловмисника, які охоплюють різні можливі випадки розвитку атаки та протиправних дій.

Іншим фактором у формуванні сценарію дій зловмисника може бути його соціалізація, зокрема, його професійний статус. Так отримуємо ще один поширений тип зловмисника – «зловмисника-виконавця», який виконує чиєсь замовлення або наказ, тобто атакуючі дії з реалізації загрози T – це його звичайна робота, яку він просто зобов'язаний виконувати. Тому в цьому випадку ймовірність активації загрози T дорівнює $P_t = 1$.

Як це витікає із формули (1), ймовірність P_T реалізації загрози T – це добуток

$$P_T = P_t P_v, \quad (8)$$

де P_v – ймовірність вдалого використання зловмисником вразливостей інформаційної системи (ІС), що містить інформаційний ресурс I, тому цілком природною є спроба економіко-вартісної інтерпретації цієї ймовірності. В загальному випадку P_v – узагальнена (інтегрована) ймовірність успішного проведення комплексу атак, породжених існуванням сукупності вразливостей ІС (включно із вразливостями самої системи захисту інформації (СЗІ)). Тобто значення ймовірності P_v залежить від ступеню захищеності ІС, який в свою чергу зумовлюється обсягом інвестувань в СЗІ (величиною c), і певним чином враховується співвідношенням [3,5]:

$$P_v = \frac{q}{q + sc}, \quad (9)$$

де s – коефіцієнт, можливий діапазон значень якого пов'язаний з існуючою у світовій практиці залежністю між рівнем інвестицій c у СЗІ та цінністю критичної інформації для її власника (сторона В). Так, для комерційної таємниці найчастіше c = (0,05÷0,20) q [1]. Зокрема для конкретних даних,

наведених у [1], маємо нижню межу для: $s \geq 10 \div 45$. З формули (6) очевидно, що за умов відсутності критичної інформації в ІС (тобто q=0) ймовірність P_v=0. При $q>>sc$, тобто при значному рівні критичності ресурсу I й низьких витратах на створення і функціонування СЗІ, наслідком чого є об'єктивна неможливість забезпечити адекватний рівень захисту критичної інформації в ІС, ймовірність $P_v \to 1$. В усіх інших випадках ймовірність Pv відмінна від 0, а її значення при $q=const$ зростає із спадом рівня інвестицій в СЗІ.

Формула (8) застосовна разом із формулами (7), (9) для обчислення P_T у випадку «зловмисника-прагматика» або «зловмисника-месника», тоді як у разі «зловмисника-виконавця» оцінювання ймовірності реалізації вразливостей виконується за виразом

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

Окремо слід зазначити, що «зловмисник-виконавець» – це як правило професіонал, який, виконуючи поставлене перед ним завдання, може, залежно від важливості цього завдання, розраховувати на залучення для підтримки своїх дій певних додаткових ресурсів: фінансових, технічних, інформаційно-аналітичних, оперативних. На практиці це означає, що у випадку «зловмисника-виконавця» існує велика ймовірність застосування для реалізації загроз високовитратних атак. Зокрема, якщо $D \to \infty$, то $P_v \to 1$, тобто можна очікувати появу дуже високих значень $P_{v\max}$.

Наведені вище формули (5) – (11) можуть бути застосовані безпосередньо для параметризації та обчислення ризиків будь-якої конкретної організації за умов, що існує реальна змога проаналізувати та кількісно оцінити економіко-вартісні характеристики реалізації загрози інформації. Вихідні данні для цих оцінок можна отримати, виконавши обстеження (аудит) стану інформаційної безпеки організації відповідно з настановами та рекомендаціями перелічених вище стандартів менеджменту ризиків за наявності певної додаткової інформації, статичні у часі оцінки (5), (6) можна розвинути у динамічні, що змінюють свої значення у часі відповідно до прийнятих економіко-вартісних сценаріїв розвитку атак [5,6].

Крім то, ці ж формули (5) – (11) дозволяють побудувати оптимізаційну схему, за якою можна буде зробити висновки щодо ефективності та доцільності інвестицій у СЗІ організації. Для цього припустимо [5], 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 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 $R = P_t P_v q$. Таким чином величина втрат, які вдалося попередити завдяки інвестуванню в СЗІ, становить

$$R_1 - R = P_t q - P_t P_v q = (1 - P_v) P_t q = P_s P_t q, \qquad (11)$$

а відповідний «прибуток» –

$$\Delta_R = R_1 - R - c = (1 - P_v) P_t q - c. \qquad (12)$$

Отримані співвідношення (11), (12) за своїм змістом тотожні формулам (2), (3), однак на відміну від останніх мають «прозору» структуру, кількісні параметри якої фактично являють собою комбінації параметрів ризику, котрі, як це вже зазначалося вище, припускають достатньо просту процедуру оцінювання безпосередньо за настановами та рекомендаціями стандартів менеджменту ризиків. Крім того, аналіз співвідношення (12) як функції змінної c та дослідження його на екстремум:

$$\frac{d\Delta_R}{dc} = \frac{s(q + sc) - s^2 c}{(q + sc)^2} P_t q - 1 = 0, \qquad (13)$$

дозволяє визначити [5] діапазон «розумних» інвестицій: $0 < c < q(P_T s - 1)/s$, обсяг інвестицій, який забезпечує найбільше значення Δ_R:

$$c_{eff} = \frac{q}{s}(\sqrt{P_t s} - 1), \qquad (12)$$

значення ймовірності P_v і ризику R для цього обсягу інвестицій:

$$P_v(c_{eff}) = \frac{1}{\sqrt{P_t s}}, \; R_T(c_{eff}) = P_v P_t q = q\sqrt{\frac{P_t}{s}}. \qquad (13)$$

Тепер, маючи значення інвестицій c_{eff}, ми можемо вважати їх своєрідним еталоном для того, щоб адекватно інвестувати в інформаційну безпеку. До речі, Гордон і Лоеб в своїх дослідженнях для достатньо загального випадку встановили, що інвестиції у захист не мають перевищувати 37% [16] від обсягу загальних збитків, а якщо бути точним, ці автори кажуть, що інвестиції мають бути набагато менші, ніж наведений відсоток. Відзначимо, що економіко-вартісні моделі «атака – захист» дають можливість на основі конкретної інформації про реальну організацію перевірити, чи достатні за обсягом кошти, інвестовані у інформаційну безпеку цієї організації, що суттєво відрізняє

економіко-вартісні моделі від моделі Гордона-Лоеба, яку практично неможливо підлаштувати під конкретику реальної організації.

Висновки. Найбільш поширеним в практиці захисту інформації методам аналізу та дослідження ризиків, наведеним в міжнародних та національних стандартах, властивий ряд вад, зокрема, занадто загальний концептуально-рекомендаційний характер подання матеріалів, що практично виключає можливість врахування при аналізі характерних специфічних властивостей об'єктів ризику й істотно зменшує об'єктивність та точність отриманих результатів. Крім того, орієнтація нових стандартів з інформаційної безпеки серії ISO 27000 на ітеративну процедуру управління ризиками за Шухартом-Демінгом обумовлює застосування переважно перебірного підходу у побудові СЗІ, звужуючи можливості застосування аналітичних оптимізаційних методів.

З іншого боку, використання відомих моделей Гордона-Лоеба для дослідження проблеми ефективності інвестування у системи захисту практично виключає можливість врахування у цих дослідженнях конкретики реального об'єкту ризику й фактично відмежовує цей підхід від прикладних досліджень реальних об'єктів ризиків. Загалом модель Гордона-Лоеба не пристосована для розв'язання прикладних вузько профільних задач.

В цій ситуації перспективним видається застосування для аналізу та дослідження інвестицій і ризиків методології, що базується на врахуванні мотиваційно-вартісних та фінансово-економічних особливостей ситуації «атака-захист» на об'єктах інформаційної діяльності через виділення низки типових сценаріїв виникнення та розвитку цієї ситуації та побудови відповідних моделей. Для ідентифікації моделей можуть бути цілком успішно використані дані та відомості, отримані за рекомендаціями та настановами міжнародних стандартів. Задля забезпечення більшої адекватності цих моделей вимогам практичного застосування до їх структури передбачено введення інформації про психо-соціальні характеристики зловмисника.

ЛІТЕРАТУРА

[1]. Андрощук Г.А., Крайнев П.П. Экономическая безопасность предприятия: защита коммерческой тайны. – К.: Изд. Дом «Ин Юре», 2000. – 400с.

[2]. Архипов А.Е. Применение среднего риска для оценивания эффективности защиты информационных систем.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.// науково-техн. зб. – Київ, 2007. – Вип. 1(14). – с.60-67.

[3]. Архипов А.Є., 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, 1(16) вип., 2008р.

[4]. Архипов А.Е. Об особенностях оценивания вероятностей, используемых для вычисления информационных рисков. // Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту: Матеріали міжнародної наукової конференції (ISDMCI '2010). Том 2. – Херсон: ХНТУ, 2010. – 590с, с.515-517.

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

[6]. Архипов А.Е. Особенности анализа рисков в информационно-коммуникационных системах // Захист інформації – 2012. – №4 (57) – С.18-27.

[7]. Левченко Є.Г., Рабчун А.О. Оптимізаційні задачі менеджменту інформаційної безпеки // Сучасний захист інформації. – 2010.- №1. – С.16-23.

[8]. Левченко Є.Г., Демчишин М.В., Рабчун А.О. Математичні моделі економічного менеджменту інформаційної безпеки // Системні дослідження та інформаційні технології. – 2011-№4. – С.88-96.

[9]. Марцынковский Д.А., «Руководство по риск-менеджменту» / Марцынковский Д.А., Владимирцев А.В., Марцынковский О.А. // Ассоциация по сертификации «Русский Регистр». – Санкт-Петербург: Береста, 2007. 10.

[10]. Олександрович Г.Я. Автоматизация оценки информационных рисков компании/ Олександрович Г.Я., Нестеров С.А., Петренко С.А // Защита информации. Конфидент. – 2003 – № 2 – С. 78-81.

[11]. Симонов С. Анализ рисков, управление рисками // JetInfo – № 1 – 1999 .

[12]. Симонов С. Технологии и инструментарии для управления рисками // Jet Info – № 2 – 2003.

[13]. AS/NZS 4360:2004 (In the form of AS/NZS ISO 31000:2009 – Principles and Guidelines on Implementation).

[14]. BS 31100:2011 Risk management. Code of practice and guidance for the implementation of BS ISO 31000.

[15]. BS 7799-3:2006 Information security management systems. Guidelines for information security risk management.

[16]. Gordon L.A., Loeb M.P. (2002), "The Economics of Information Security Investment", ACM Transaction on Information and System Security, Vol.5, No4, pp.438-457.

[17]. Huang, C.D./ Hu, Q., and Behara, R.S., Economics of Information Security Investment in the Case of Simultaneous Attacks, Proceedings of the Fifth

Workshop on the Economics of Information Security. June 26-28, 2006, Cambridge, England.
[18]. ISO/IEC 16085:2006 Systems and software engineering – Life cycle processes - Risk management.
[19]. ISO/IEC 17799:2005 – Information technology – Security techniques – Code of practice for information security management.
[20]. ISO/IEC 27005 – Information security risk management.
[21]. ISO/IEC TR 13335-3:1998 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security.
[22]. ISO/IEC TR 13335-4:2000 Information technology - Guidelines for the management of IT Security – Part 4: Selection of safeguards.
[23]. LAWRENCE A. GORDON and MARTIN P. LOEB "The Economics of Information Security Investment" ACM Transaction on Information and System Security, Vol.5, No4, November 2002, Pages 438-457.
[24]. NIST Special Publication 800-30 – Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards.
[25]. Willemson J., Extending the Gordon&Loeb Model for Information Security Investment. The Fifth International Conference on Availability, Reliability and Security ARES 2010, IEEE, 2010.

REFERENCES

[1]. Androschuk G.A, Kraynev P.P. (2000), "Economic safety of company: Security of commercial information", K. Ed. House" Eun Ure.
[2]. Arhypov A.E. (2007), "Application of average risk for assessment of effectiveness of information systems", Legal, regulatory and metrology systems of information security in Ukraine, Issue 1(14), pp.60-67.
[3]. Arhypov A.E., Arhypova A.S. (2008), "Application of motivational-cost models for descriptions of probability value in the system" attack – defense", Legal, regulatory and metrological assurance of information security in Ukraine, Vol. 1(16).
[4]. Arhypov A.E. (2010), "About the features of estimation the probabilities used to calculate information risks", Intelligent Decision Support Systems and Problems of Computational Intelligence: Proceedings of the International Scientific Conference (ISDMSI '2010), Vol2., pp.515-517.
[5]. Arhypov A.E. (2011), "Application of economic and motivational-cost for descriptions of probability value of information risks", Information Security, Vol.2 (51), pp.69-76.
[6]. Arhypov A.E. (2012), "Features of the analysis of risks in information and communication systems", Information Security, Vol.4 (57), pp.18-27.
[7]. Levchenko E.G., Rabchun A.O. (2010), "Optimization problem of information security management", Modern information security, Vol.1, pp.16-23.
[8]. Levchenko E.G., Demchishin M.V., Rabchun A.O. (2011), "Mathematical model of economic management of information security", System Research and Information Technology, Vol.4, pp.88 -96.
[9]. Martsynkovsky D.A., Vladimirtsov A.V., Martsynkovsky O.A. (2007), "Guide to Risk Management", Association of certification for "Russian Rehystr".
[10]. Oleksandrovych G.Y, Nesterov S.A., Petrenko S.A. (2003), "Automation Location of information risks", Information Security.Konfydent, Vol.2, pp. 78-81.
[11]. Simonov S. (2003), "Risk Analysis, Risk Management", Jet Info Vol.1.
[12]. Simonov S. (2003), "Technology and instruments for Risk management", Jet Info Vol.2.
[13]. AS/NZS 4360:2004 (In the form of AS/NZS ISO 31000:2009 - Principles and Guidelines on Implementation).
[14]. BS 31100:2011 Risk management. Code of practice and guidance for the implementation of BS ISO 31000.
[15]. BS 7799-3:2006 Information security management systems. Guidelines for information security risk management.
[16]. Gordon L.A., Loeb M.P. (2002), "The Economics of Information Security Investment", ACM Transaction on Information and System Security, Vol.5, No4, pp.438-457.
[17]. Huang, C.D./ Hu, Q., and Behara, R.S., Economics of Information Security Investment in the Case of Simultaneous Attacks, Proceedings of the Fifth Workshop on the Economics of Information Security. June 26-28, 2006, Cambridge, England.
[18]. ISO / IEC 16085:2006 Systems and software engineering - Life cycle processes - Risk management.
[19]. ISO / IEC 17799:2005 - Information technology - Security techniques - Code of practice for information security management.
[20]. ISO / IEC 27005 - Information security risk management.
[21]. ISO / IEC TR 13335-3:1998 Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security.
[22]. ISO / IEC TR 13335-4:2000 Information technology - Guidelines for the management of IT Security - Part 4 : Selection of safeguards.
[23]. LAWRENCE A. GORDON and MARTIN P. LOEB "The Economics of Information Security Investment" ACM Transaction on Information and System Security, Vol.5, No4, November 2002, Pages 438-457.
[24]. NIST Special publication 800-30 - Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards.
[25]. Willemson J. (2010), "Extending the Gordon & Loeb Model for Information Security Investment", The Fifth International Conference on Availability, Reliability and Security ARES 2010, IEEE, 2010.

ИНФОРМАЦИОННЫЕ РИСКИ: МЕТОДЫ И СПОСОБЫ ИССЛЕДОВАНИЯ, МОДЕЛИ РИСКОВ И МЕТОДЫ ИХ ИДЕНТИФИКАЦИИ

Рассматриваются нормативно-правовые документы в области информационной безопасности, методы оценки информационных рисков, в частности экономико-стоимостные модели для идентификации вероятностных параметров и структуры информационных рисков, применение этих моделей для анализа инвестиций в информационную безопасность. Обычно для проведения адекватного оценивания информационных рисков и оптимизация объемов инвестиций в информационную безопасность применяются подходы и процедуры, опирающиеся на существующие международные стандарты по менеджменту рисков информационной безопасности. К сожалению, эти стандарты имеют преимущественно концептуально рекомендательный характер и не учитывают многих факторов, которые существенно влияют на точность и объективность оценки рисков. Экономико-стоимостной подход к анализу рисков, в частности известная модель Гордона-Лоэба, ориентированы преимущественно на исследование оптимизационных аспектов управления рисками, однако практически исключают возможность учета в этих исследованиях конкретики реального объекта риска. Предложены модели, которые используют эвристические мотивационно-стоимостные механизмы определения параметров и структуры рисков. Данные модели позволяют объединить изложенные в международных стандартах методы анализа и оценки рисков с возможностями оптимизационных исследований риска, заложенных в модели Гордона-Лоэба. Для обеспечения большей адекватности этих моделей требованиям практического применения предусмотрено введение в их структуру информации о психо-социальные характеристики злоумышленника.

Ключевые слова: Информационная безопасность, стандарты по менеджменту рисков информационной безопасности, методы оценки рисков, исследование инвестиций в информационную безопасность, психотипы злоумышленников.

INFORMATION RISK: RESEARCH METHODS AND TECHNIQUES, MODELS AND METHODS OF RISK IDENTIFICATION

Legal documents in the field of information security, information risk assessment methods are considered, including economic-cost models to identify the probability parameters and structure of information risks, and applying these models to analyze investment in information security. Of course, for an adequate assessment of information risks and optimizing investments in information security used approaches and procedures, which are based on existing international standards of information security risk management. Unfortunately, these standards are more conceptual and advisory in nature. Based on this situation, many factors aren't considered into account, which significantly affects the accuracy and objectivity of risk assessment. Economic-cost approach for analysis of risks, including well-known model of Gordon-Loeb, is focused mainly on the study of optimization aspects of risk management, but virtually eliminates the possibility of considering into account the specificity of these studies, the risk of a real object. It's suggested that models, which use heuristic cost-motivational mechanisms to determine the parameters and structure of risks. These models allow combining methods of analysis and risk assessment methods, which are set out in international standards, with the possibilities of optimization researches of risk, inherent in the Gordon-Loeb model. In order to ensure more adequacy of these models to requirements of practical application, it's proposed to input into their structure the psycho - social characteristics of the attacker.

Keywords: Information security, standards of risk management of information security, risk assessment methods, research investment in information security, psycho of attackers.

Олександр Євгенійович Архипов, доктор технічних наук, професор кафедри інформаційної безпеки НТУУ «КПІ»
E-mail: sonet@zeos.net
Александр Евгеньевич Архипов, доктор технических наук, профессор кафедры информационной безопасности НТУУ «КПИ»
Oleksandr Arkhypov, Dr. Sci. Tech., professor at the Department of Information Defense at National Technical University of Ukraine "Kyiv Polytechnic Institute".

Андрій Володимирович Скиба, магістр НТУУ «КПІ»
E-mail: andrewskyba@ukr.net
Андрей Владимирович Скиба, магистр НТУУ «КПИ»
Andrii Skyba, M.S. NTUU "KPI"