УДК 004.056.5:658.1

А. В. Бєгун,
к. е. н., доцент, доцент кафедри інформаційного менеджменту,
Київський національний економічний університет імені Вадима Гетьмана

ОЦІНКА ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

A. Biegun,
Ph. D. associate Professor of the Department of information management,
Kyiv National Economic University named after Vadym Hetman

ASSESSMENT OF ECONOMIC EFFICIENCY OF THE ENTERPRISE INFORMATIONAL SECURITY

Стаття присвячена аналізу показників економічної ефективності систем інформаційної безпеки в процесі розвитку підприємства. Цей процес повинен існувати в умовах збалансованого дійства: безпека — витрати.

The article is devoted to the analysis of indicators of economic efficiency of information security systems in the process of development of the enterprise. This process should exist in the conditions of balanced action: security — expenditures.

Ключові слова: економічна ефективність, безпека, відвернутий збиток, понесений збиток, система захисту інформації, загрози.

Key words: economic efficiency, safety, prevented damage suffered damage, the system of protection of information threats.

ВСТУП

Необхідність залучення технологій інформаційної безпеки високого рівня і особливо до збереження конфіденційних даних економічних процесів ініціювала появу на ринку не лише самих засобів захисту, але і систем управління цими засобами: побудова процесів управління інцидентами, конфігураціями і засобами їх автоматизації. Водночас світовий бізнес почав висувати підвищені вимоги до візуалізації засобів аналізу, моніторингу і створення єдиного центру управління інформаційною безпекою в кожній компанії. За таких умов проявилися деякі загальні тенденції розвитку ринку засобів безпеки. По-перше, бізнес має інтерес не тільки з приводу дотримання законодавства у сфері ІБ, а і з приводу того, що дає ІБ бізнесу. Іншою загальносвітовою тенденцією є галузева стандартизація у сфері ІБ. Наприклад, постанова НБУ № 474 від 28.10.2010 року, за якою банки повинні впровадити систему управління інформаційною безпекою (СУІБ) у відповідності до стандартів НБУ і розробити систему відповідальності за умов невиконання цього стандарту. Третім фактором, що визначає майбутнє ринку ІБ, є поява "хмарних обчислень" (cloud computing) — технології розподільної обробки даних, у якій інформаційні ресурси і потужності надаються користувачеві як інтернет-сервіс.

Інформаційне середовище підприємства незалежно від свого складу обов'язково повинне передбачати систему безпеки. Однак витрати на забезпечення високого рівня такої системи безпеки можуть бути занадто високими. Тому знаходження розумного компромісу, вибір раціонального рівня інформаційної безпеки (ІБ) в умовах коливання витрат є обов'язковою складовою економічної ефективності безпеки підприємства.

Оцінка систем безпеки та системних характеристик на різноманітних рівнях (якісному, кількісному) досліджувалася в роботах [4—5,7—8]. Але обчислення таких показників як ризик, надійність, гнучність та керованість систем захисту інформації не завжди відповідає економічним характеристикам ефективності діяльності підприємства в умовах постійного розвитку інформаційних технологій, комунікацій та засобів, які їх підтримують [2—3].

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Визначити показники ефективності систем інформаційної безпеки підприємства достатньо складно. Це пояснюється важливістю задач, які виконуються в процесі забезпечення ІБ, кінцевим результатом діяльності підприємства, складністю виміру їх з витратами, різноманітними методами і видами забезпечення, специфікою економічних відносин.

Доцільність використання ресурсного забезпечення пропонує виконання системою ІБ сукупності дій (рішень), які спрямовані на досягнення оперативних та стратегічних цілей. В свою чергу, цілі системи ІБ досягаються в декілька етапів і деякими підсистемами. Виконання запропонованих дій з досягнення цілей має результат — ефект у вартісних або натуральних вимірах. Тоді економічна ефективність ІБ — співвідношення між економічним ефектом й витратами ресурсів, які необхідні для забезпечення відповідного рівня ІБ підприємства.

Стосовно [1], [6], під економічною ефективністю безпеки розуміється відношення відвернутого збитку до витрат на її забезпечення. Але відвернутий збиток — це не єдиний результат діяльності системи безпеки. До того ж слід враховувати, що 100% захисту неможливо досягти; існує остаточний ризик реалізації загрози, який прогнозує можливість збитку — від'ємного результату. Таким чином, ефектом дій із забезпечення ІБ є відвернутий та понесений збиток у вартісному вигляді.

Тоді рівень економічної ефективності ІБ буде визначатися за формулою

$$E_{eco} = (U_{if} — U_{inf}) / Z_0 \quad (1),$$

де U_{if} — відвернутий збиток, тобто можливий збиток в результаті атаки на інформаційну систему;

U_{inf} — збиток від реалізації атаки на інформаційну систему;

Z_0 — витрати на забезпечення інформаційної безпеки.

Враховуючи формулу $U_{inf} = U_{inf/st} + U_{inf/ind}$ ($U_{inf/st}$ — прямі збитки, $U_{inf/ind}$ — непрямі збитки), розрахунок E_{eco} має наступний вигляд:

$$E_{eco}* = (U_{if} — U_{inf}) / (Z_f + Z_s + Z_y) \quad (2),$$

де Z_f — витрати на формування політики інформаційної безпеки;

Z_s — витрати на відповідність політики інформаційної безпеки;

Z_y — витрати, які пов'язані з наслідками порушення політики інформаційної безпеки.

Тут необхідно враховувати страхування залишкового інформаційного ризику: величина страхового внеску (s) збільшить

величину витрат (Z_0), а страхові виплати у випадку настання страхової події (S) зменшать розмір збитку (U_{inf}):

$$E_{eco} = (U_{if} — U_{inf} + s) / (Z_0 + s) \quad (3).$$

Оптимізація абсолютної економічної ефективності можлива при

$$U_{if} -> MAX,$$
$$U_{inf} -> MIN, \quad (4).$$
$$Z_0 -> MIN.$$

Мінімізація можливого збитку і максимізація відвернутого збитку — це задачі, які необхідно розв'язувати в комплексі. Так, необгрунтована економія витрат при збереженні попередніх показників U_{if} та U_{inf} може в подальшому призвести до обвалу всієї системи захисту інформації. На практиці існують випадки завищення показників U_{if} і заниження U_{inf} для того, щоб представити в найбільш привабливому вигляді діяльність служби інформаційної безпеки.

Розрахунок відвернутого збитку повинен базуватися на існуванні спроби (факту) інформаційної атаки, яка своєчасно була визначена й ліквідована. Тоді ефект інформаційної безпеки буде вимірюватися вартістю збереженого та збільшеного інформаційного ресурсу (C_{inf}):

$$E_{eco}** = C_{inf}/Z_0 \quad (5).$$

Але наявність надлишкового інформаційного ресурсу повинна мати певний рівень кореляції з показниками чистого прибутку підприємства або можливості його отримання. Визначимо комерційну ефективність ІБ, як

$$E_{com} = PP/Z_0 \quad (6),$$

де PP — величина чистого прибутку підприємства.

Оцінка збитків у випадку реалізації атаки на систему захисту інформації відбувається за допомогою експертів і розглядається як інформаційний ризик:

$$R_{inf} = P_{inf} \cdot U_{inf} \quad (7),$$

де R_{inf} — інформаційний ризик,

P_{inf} — ймовірність реалізації інформаційної атаки,

U_{inf} — збиток, отриманий в результаті реалізації атаки.

Насправді збиток визначається не тільки прямими, але й непрямими втратами. На практиці неможливо точно обчислити непрямі витрати такі, як зниження довіри користувача до продукції та послуг підприємства тощо.

Оцінювання ефективності систем захисту інформації крім запропонованих розрахунків комерційної та економічної ефективності систем безпеки повинне враховувати кінцеві цілі й вимоги, які притаманні сучасним системам інформаційної безпеки. Серед таких вимог найбільш важливі — оснащення сучасними технічними засобами й наявність висококваліфікованих фахівців.

Важливою умовою існування ефективної системи інформаційної безпеки підприємства є правильна організація аудиту, який не повинен наносити шкоду підприємству. Тому тут дійсно необхідні такі важелі, як неочікуваність, обгрунтованість етапів аудиту, використання сучасних стандартів, технологій і кваліфікованих фахівців. Все це можливо при наявності відповідних ресурсів для проведення аудиту.

Найбільш дієздатним методом аудиту систем інформаційної безпеки є перевірка системи на відповідність міжнародним стандартам ІБ та ігрового підходу на вразливість й стійкість. Такий підхід дозволяє виявити ефективність діяльності системи за плановими та фактичними показниками:

$$Aud = E_{plan}/E_{fact}.$$

Якщо $Aud > 1$, то система захисту інформації має запас надійності, але є надмірною; при $Aud < 1$ — до системи слід вносити корегування: в саму систему захисту інформації, організацію системи інформаційної безпеки та систему управління економічною безпекою підприємства.

ВИСНОВКИ

Запропоновані в дослідженні формули розрахунків рівня ефективності можна модифікувати та використовувати при обгрунтуванні організації та модернізації системи управління економічною безпекою підприємства. Але при цьому слід враховувати наступне:

— збитки при реалізації атак на систему інформаційної безпеки будуть зменшувати прибуток;

— страхування у випадку відсутності та слабкості системи захисту інформації буде недоцільним, виняток — страхування від стихійних лих;

— обгрунтування організації захисту інформаційних ресурсів повинно проводитися на перспективу не менш 3-х років, витрати на формування і реалізацію політики інформаційної безпеки великі, а ефект не може бути тимчасовим.

Література:

1. Андрианов В.В. Обеспечение информационной безопасности бизнеса/В.В. Андрианов, С.А. Зефиров, В.Б. Голованов, Н.А. Голдуев. — 2-е изд., перераб. и доп. — М.: ЦИПС и Альшина Паблишерз, 2011. — 373 с.

2. Бєгун А.В. Інформаційна парадигма безпеки економічної системи // Моделювання та інформаційні технології в економіці. — № 83. — 2011. — С. 144—151.

3. Бєгун А.В. Аспектно-орієнтована технологія оптимізації захисту додатків Web-порталу // Моделювання та інформаційні технології в економіці. — № 81. — 2010. — С. 189—196.

4. Бєгун А.В. Модель оцінювання ефективності захисту інформаційних ресурсів банку // Сб. научн. труд. "Анализ, моделирование, управление, развитие экономических систем". — Симферополь: ТНУ. — 2012. — С. 51—53.

5. Бєгун А.В., Ігнатова Ю.В. Оцінка методів дослідження системних характеристик діяльності елеватора // Моделювання та інформаційні технології в економіці. — № 88. — 2013. — С. 121—132.

6. Валдайцев С.В. Оценка бизнеса и управление стоимостью предприятия: Учебное пособие. — М.:ЮНИТИ-ДАНА, 2001. — 720 с.

7. Светлаков Е.С. Экономическая безопасность предприятия. — Защита информации. — Конфидент. — № 3. — 2002. — С. 51—55.

8. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративних сетях и системах. — Москва: ДМК, 2002 г. — 656 с.

References:

1. Andrianov, V. (2011), Obespechenie informacionnoj bezopasnosti biznesa [Providing business information security], 2nd ed, CIPS i Al'shina Pablisherz, Moscow, Russia.

2. Biegun, A. (2011), "Informational paradigm of security economic system", Modeliuvannia ta informatsijni tekhnolohii v ekonomitsi, vol. 83, pp. 144—151.

3. Biegun, V. (2010), "Aspect-oriented technology optimization of protection applications Web-portal", Modeliuvannia ta informatsijni tekhnolohii v ekonomitsi, vol. 81, pp. 189—196.

4. Biegun, V. (2012), "Model evaluation of the effectiveness of protection information resources of the bank", Sbornik nauchnyh trudov "Analiz, modelirovanie, upravlenie, razvitie jekonomicheskih sistem", pp. 51—53.

5. Biegun, V. and Ignatova, Y. (2013), "Assessment of the research methods of system characteristics of activity of the Elevator", Modeliuvannia ta informatsijni tekhnolohii v ekonomitsi, vol. 88, pp. 121—132.

6. Waldaycev, S. (2001), Ocenka biznesa i upravlenie stoimost'ju predprijatija: Uchebnoe posobie [Business valuation and management of enterprise value: a Training manual], UNITY-DANA, Moscow, Russia.

7. Svetlakov, Y. (2002), "Economic safety of the enterprise. Protection of information", Confident, vol. 3, pp. 51—55.

8. Sokolov, A.V. and Shangin, V.F. (2002), Zashhita informacii v raspredelennyh korporativnih setjah i sistemah [Information security in distributed corporate networks and systems], DMK, Moscow, Russia.

Стаття надійшла до редакції 29.09.2013 р.