Ліпський С.В.
ст. гр. ОМОм-11,
Шухманн В.А.
Науковий керівник: Мельник Н.Г., к.е.н., доцент,
кафедра обліку в державному секторі економіки та сфері послуг,
Тернопільський національний економічний університет,
м. Тернопіль, Україна

ЕКОНОМІЧНА СУТНІСТЬ ВИТРАТ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

У сучасних умовах інформація набуває все більшого значення для функціонування та розвитку суб'єктів господарювання. Саме інформація є одним із найважливіших ресурсів у розвитку підприємства та охоплює нові ідеї і технології, комерційні та інноваційні проекти, аналітичні розробки, виробничі плани та звітність, тому поряд із завданнями ефективної обробки й передачі інформації, забезпечення надійності захисту інформаційних ресурсів є однією з головних задач сучасного бізнесу є управління інформаційними ризиками [1].

Як зазначають В. В. Волкова, М. Р. Васютенко, серйозна увага до питань інформаційної безпеки спричинює проблему оцінки рівня безпеки інформаційних систем підприємства, визначення величини грошових коштів, які потрібно виділити на вирішення проблем інформаційної безпеки, розподілу грошових коштів між засобами, які забезпечують захист інформації, зниження інформаційних ризиків. Найчастіше зазначені проблеми розв'язують на інтуїтивному рівні, без обґрунтування фінансової доцільності рішень, адже керівництво підприємств не завжди оцінює важливість цього питання та має інформацію про співвідношення витрат на забезпечення інформаційної безпеки та збитків від втрати інформації. Іноді на інформаційній безпеці економлять, хоч це найчастіше призводить до істотних фінансових і моральних втрат, які можуть бути причиною краху підприємства [1].

Витрати на інформаційну безпеку у всьому світі суттєво зростають з року в рік. Зокрема, за оцінками експертів, у 2016 році такі витрати зросли на 7,9% і досягли 81,6 мільярдів доларів. Основні витрати, що виникають у цій сфері, припадають на консалтинг та аутсорсинг. До кінця 2020 року обсяг ринку систем інформаційної безпеки може сягнути 170 млн.$, а найвищі темпи зростання будуть на витрати з тестування безпеки, аутсорсинг послуг і рішень для захисту від витоку конфіденційної інформації (Data Loss Prevention – DLP) [2].

Високі темпи будуть спостерігатися у сегменті безпеки управлінських рішень. В той же час, рішення, такі як SIEM (Security Information and Event Management – управління інформаційною безпекою та подіями безпеки) і SWG (Secure Web Gateways – безпечні веб-шлюзи) за прогнозами аналітиків також будуть успішно розвиватися.

Згідно з оцінками компанії Gartner (провідна світова дослідницька і консалтингова компанія у сфері інформаційних технологій) в період до 2020 року, у сфері SWG буде ріст продаж в середньому на 5-10% річних. Причиною такого зростання є те, що підприємства все частіше звертають увагу на рішення для виявлення і реагування на інциденти, тому, що превентивні підходи не завжди спрацьовують і дають правильний результат у блокуванні злочинних атак на інформаційні ресурси компаній [2].

Аналітична компанія IDC прогнозує, що швидке зростання цифрових технологій змушує компанії у всіх країнах світу інвестувати в безпеку для захисту від відомих і невідомих загроз. На глобальному рівні в період 2015-2020 років найбільше на програмне забезпечення й послуги захисту будуть витрачати банки, дискретні виробництва та організації, пов'язані з органами влади. Разом ці три сектори забезпечать в межах 30% світових доходів на інформаційну безпеку в 2017 році [3].

За прогнозами IDC, інші три сектори – безперервне виробництво, професійні послуги та телекомунікації будуть витрачати у 2017 року в межах 5 млрд. $ на продукти, які пов'язані з безпекою. Найбільшим ринком витрат на інформаційну безпеку залишиться США (36,9 млрд. доларів в 2017 році), Західна Європа (19,2 млрд. доларів), Азіатсько-Тихоокеанський регіон (за винятком Японії) – 18,5%. Дві третини витрат припадають на компаній пов'язані з великим бізнесом, мультинаціональними корпораціями [3].

При розробці системи захисту інформації на будь-якому підприємстві виникають витрати, які є необхідними та неминучими. Необхідні витрати – це ті, які необхідні, навіть якщо рівень загрози безпеці підприємства є досить низьким. Це витрати на технічне обслуговування досягнутого рівня безпеки інформації компанії. До неминучих витрат можна віднести: обслуговування технічних засобів захисту; конфіденційне діловодство; функціонування та аудит безпеки; мінімальний рівень перевірки та контролю через спеціалізовані організації (аутсорсинг); підготовка кадрів до застосування методів інформаційної безпеки.

Методика оцінки сукупної вартості витрат на інформаційну безпеку була запропонована аналітичною компанією Gartner наприкінці 80-х років (1986-1987), і дозволяла оцінити вартість інформаційних технологій. Методологія компанії Gartner дозволяє обчислити всі витрати в частині інформаційних активів компанії, у тому числі прямих і непрямих витрат на устаткування та програмного забезпечення, організаційні заходи, навчання та підвищення кваліфікації співробітників компанії, реорганізації, реструктуризації бізнесу та ін. [4].

Цей метод можна використовуватися для доказу економічної ефективності існуючих корпоративних інформаційних систем захисту. Це дозволяє менеджерам служб обґрунтовувати бюджет витрат на інформаційну безпеку, а також довести ефективність роботи працівників служби безпеки. Оскільки оцінювання економічної ефективності корпоративних інформаційних систем захисту стає «вимірюваним» – це дозволяє вирішувати завдання моніторингу і корекції показників економічної ефективностіі, зокрема, сукупної вартості витрат. Таким чином, величину витрат можна використовуватися як інструмент для оптимізації затрат на забезпечення необхідного рівня безпеки та обґрунтування бюджету.

Загалом, методика оцінки витрат, запропонована компанією Gartner, дозволяє [4]:

– отримати адекватну інформацію про рівень безпеки IT компанії та загальну вартість корпоративних інформаційних систем захисту;

– порівняти служби інформаційного захисту як між собою, так і з іншими службами компанії;

– оптимізувати інвестиції в інформаційну безпеку компанії з урахуванням реальної вартості сукупних витрат.

Вартість системи інформаційної безпеки в залежності від конкретних вимог для режиму безпеки інформації, повинна бути близько 10-20% від вартості комп’ютерної інформаційної системи підприємства в цілому.

Список використаних джерел

1. Волкова В. В. Визначення витрат на забезпечення інформаційної безпеки підприємства на засадах математичного моделювання // В. В. Волкова, М. Р. Васютенко [Електронний ресурс]. – Режим доступу: http://www.vestnikdnu.com.ua/archive/201482/222.html
2. Расходы на информационную безопасность [Електронний ресурс]. – Режим доступу: http://safe.cnews.ru/news/top/2016-08-09_rashody_na_ib_vyrastut_na_79_v_2016_g
3. Информационная безопасность (мировой рынок) [Електронний ресурс]. – Режим доступу: http://www.tadviser.ru/index.php

4. Информационная безопасность: экономические аспекты [Електронний ресурс]. – Режим доступу: http://masters.donntu.org/2009/fvti/khimka/library/2003_10.pdf
5. Сисюк С. В. Витрати на управління: історія розвитку облікової категорії / С. В. Сисюк, Н. Г. Мельник // Вісник Житомирського державного технологічного університету / Економічні науки. − Житомир : ЖДТУ № 4(62). – 2012.– С.217-219.
6. Яцишин, С. Р. Розвиток та економічний зміст категорії витрати виробництва / Світлана Яцишин // Українська наука: минуле, сучасне, майбутнє. Щорічник. Випуск 8. – Тернопіль : Економічна думка, 2003. – С. 149-152.