Шевченко С. Ю.,
канд. екон. наук,
ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана», Україна

Shevchenko S. Y.,
PhD in Economics,
Kyiv National Economic University, Ukraine

ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті узагальнено сутність системи управління інформаційною безпекою підприємства, наведено основні цілі та складові елементи. Розглянуто питання економічного обґрунтування витрат на захист інформації.

SYSTEM MANAGEMENT FORMATION OF INFORMATION SECURITY OF COMPANY

The article generalizes the essence of the system management formation of company information security, adduces its main aims and elements. It is also devoted to the issue of economic reasoning of expenditure on protection of information.

В умовах економіки постіндустріального суспільства, інформація, що стосується усіх напрямків діяльності підприємства, стає найбільш цінним і дорогим ресурсом, а проблеми інформаційної безпеки — усе більш складними і практично значущими. Інформаційна безпека є однією із складових частин економічної безпеки, яка формує модель захищеності підприємства.

Різнобічному дослідженню питання забезпечення інформаційної безпеки присвячено праці С. Арзуманова, В. Домарєва, Є. Степанова, С. Петренка, О. Юдіна та ін.

Метою даного дослідження є обґрунтування пріоритету створення та управління системою інформаційної безпеки в контексті забезпечення економічної безпеки підприємства.

Згідно з міжнародним стандартом [9], система управління інформаційною безпекою — це «частина загальної системи управління організації, що заснована на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід та вдосконалення інформаційної безпеки». Серед основних її цілей можна виділити: забезпечення безпеки найважливішої корпоративної інформації; захист основних активів і критичних бізнес-процесів організації; мінімізація ризиків інформаційної безпеки при веденні операційної діяльності організації; забезпечення безперервності основної діяльності організації; підвищення загального рівня управління організації.

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують враз-

ливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою — комплексність. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Слід зазначити, що ключовим фактором, у забезпеченні інформаційної безпеки підприємства є його персонал. Основними заходами при роботі з яким є: проведення аналітичних процедур при прийомі і звільненні; навчання і інструктаж практичним діям по захисту інформації; контроль за виконанням вимог по захисту інформації, стимулювання відповідального відношення до збереження інформації та ін.

Не менш важливим є питання економічного обґрунтування витрат на захист інформації. Адже чим вище рівень захищеності інформації, тим за інших рівних умов, буде нижче розмір можливих збитків, але тим вищою буде вартість захисту. Оптимальний розміром витрат на захист буде такий, при якому забезпечується рівень захищеності, що дорівнює мінімуму загальних витрат. Вартість збитків визначається двома параметрами: ймовірністю реалізації різних загроз інформації; вартістю (важливістю) інформації, захищеність якої може бути порушена під впливом різних загроз. У зв'язку зі складністю дати кількісну оцінку збитків (сума втрат або розмір недоотриманого прибутку) причиною яких може бути витік, або втрата інформації, що захищається, в даний час найбільш доцільним є підхід на основі експертних оцінок. За даними висновків експертів можуть бути отримані статистично стійкі оцінки можливого збитку.

Захист інформаційних ресурсів підприємства є одним з ключових завдань в умовах підвищення рівня внутрішніх і зовнішніх загроз інформаційної безпеки, що можуть безпосередньо вплинути на його фінансову діяльність і стійкість на ринку. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. Сутність викладеного дає підстави стверджувати, що в сучасних умовах, без належного захисту інформаційного середовища підприємства не можливо забезпечити його економічну безпеку.

Література

1. *Арзуманов С. В*. Оценка эффективности инвестиций в информационную безопасность // Защита информации. Инсайд. — 2005. — № 1. — С. 26—25.

2. *Богуш В. М., Юдін О. К.* Інформаційна безпека держави. — К.: «МК-Прес», 2005. — 432 с.

3. *Домарев В. В*. Безопасность информационных технологий. Системный подход. — К.: ООО «ТИД «ДС», 2004. — 992 с.

4. *Донець Л. І., Ващенко Н. В*. Економічна безпека підприємства: Навч. пос. — К.: Центр учбової літератури, 2008. — 240 с.

5. *Конев И., Беляев А*. Информационная безопасность предприятия. — СПб.: БХВ Петербург, 2003. — 752 с.

6. *Корнеев И. К., Степанов Е. А*. Защита информации в офисе: учеб. — М.: ТК Велби, Изд-во Проспект, 2008. — 336 с.

7. *Петренко С., Симонов С., Кислов Р*. Информационная безопасность: экономические аспекты http://www.citforum.ru/security-/articles/sec/index.shtml

8. *Теренин А. А*. Проектирование экономически эффективной системы информационной безопасности // Защита информации. Инсайд. —-2005. — № 1. — С. 23—25.

9. ISO/IEC 17799:2005 RU; ISO/IEC 27001:2005 RU. http://iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1/