УДК 65.012.8

Шиптицька І. І.
студент,
Львівський державний університет безпеки життєдіяльності
Кухарська Н. П.
кандидат фізико-математичних наук, доцент
Львівський державний університет безпеки життєдіяльності

ОБГРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБЛЕННЯ ОРГАНІЗАЦІЯМИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В умовах, коли нематеріальні активи підприємств, які існують зазвичай у вигляді інформації, мають дедалі більший вплив на розвиток бізнесу, його конкурентоздатність, управління інформаційною безпекою (ІБ) стає невід'ємною складовою загальної системи управління організацією. Значущість систематичної цілеспрямованої діяльності щодо забезпечення інформаційної безпеки залежить від ступеня автоматизації бізнес-процесів організації і є тим вищою, чим більша частка "інтелектуальної складової" в її кінцевому продукті, чим більша залежність діяльності підприємства від забезпечення конфіденційності певної інформації (технологій, ноу-хау, комерційних баз даних, маркетингової інформації, результатів наукових досліджень тощо).

Управління інформаційною безпекою на кожному конкретному підприємстві повинно здійснюватися в контексті його загальної господарської діяльності з урахуванням характеру функціонування компанії (технологій виробництва, специфіки ринків збуту, тощо), ситуації, що фактично склалася в ринковій конкурентній боротьбі, в державній політиці, а також з врахуванням розвитку правової і правоохоронної системи, рівня розвитку використовуваних інформаційних і телекомунікаційних технологій та інших чинників, що мають вплив на поточну діяльність організації.

Для нейтралізації існуючих загроз і забезпечення ІБ на підприємствах

слід створити систему менеджменту інформаційної безпеки, яка включає:

- формування та практичну реалізацію комплексної багаторівневої політики інформаційної безпеки підприємства та системи внутрішніх вимог, норм і правил;
- організацію департаменту (служби, відділу) інформаційної безпеки;
- розроблення системи заходів і дій на випадок виникнення непередбачуваних ситуацій (“управління інцидентами”);
- проведення аудитів (комплексних перевірок) стану інформаційної безпеки на підприємстві.

Кожен з цих напрямків організаційної роботи має свої особливості і повинен реалізовуватися з використанням специфічних методів менеджменту та відповідно до встановлених міжнародними стандартами правил.

Розглянемо більш детально політику інформаційної безпеки.

Згідно визначення, поданому у стандарті “Помаранчева книга” (Trusted Compute System Evaluation Criteria), політика інформаційної безпеки (ПолІБ) – це набір норм, правил і практичних прийомів, котрі регулюють управління, захист і розподіл цінної інформації [1].

Можна навести декілька вагомих аргументів на користь необхідності розробки політики інформаційної безпеки для організації будь-якого масштабу і виду діяльності. По-перше, ПолІБ є основою для захисту всіх активів організації, що мають вплив на забезпечення ІБ, в її рамках визначаються правила розмежування доступу до цих активів. Вона визначає, яка поведінка по відношенню до активів є дозволеною, тобто санкціонованою, а яка є забороненою, несанкціонованою і свідчить про незаконне їх використання. По-друге, політика інформаційної безпеки формує “правила гри” для всіх працівників організації та третіх осіб, що дає змогу досягнути згоди стосовно питань забезпечення ІБ як всередині самої організації (включаючи її керівництво), так і зовні. По-третє, ПолІБ допомагає зробити правильний вибір платформи для роботи з активами із врахуванням інструментальних засобів і процедур, що будуть використовуватися.

Серед інших причин, що спонукують організацію розробляти політику інформаційної безпеки, виокремимо такі:

Вимоги керівництва підприємства. Декілька серйозних інцидентів, що призвели до зупинки або сповільнення роботи компанії у результаті різних локальних і віддалених атак, розголошення конфіденційної інформації чи крадіжки комп'ютерів з цінною інформацією суттєво стимулюють появу такої ініціативи з боку керівництва.

Вимоги законодавства та стандартів у сфері інформаційної безпеки. Політика інформаційної безпеки дає змогу визначити правила, у відповідності до яких частина інформації підприємства може буде віднесена, наприклад, до категорії комерційної таємниці, а це дасть можливість захистити її юридично.

Вимоги клієнтів і партнерів щодо юридичного підтвердження в контрактах та договорах необхідного рівня забезпечення ІБ, як гарантію того, що їх конфіденційна інформація також буде захищена належним чином. Саме наявність ПолІБ є переконливим доказом намірів організації відносно забезпечення інформаційної безпеки.

Підвищення інвестиційної привабливості організації. Наявність ПолІБ позиціонує організацію як таку, що є "відкрита" для інвестицій.

Необхідність сертифікації за стандартами (наприклад, ISO/IEC 9001, 27002, 15408 і т.п.), що свідчитиме про необхідний рівень забезпечення ІБ в організації.

Усунення зауважень аудиторів і виконання їх рекомендацій. Будь-яка зовнішня аудиторська перевірка, у першу чергу, звертає увагу на необхідність формалізації всіх бізнес-процесів, в тому числі особливу увагу приділяє наявності в організації ПолІБ, на відповідність якій може проводитися аудит.

Забезпечення конкурентоздатності за рахунок оптимізації бізнес-процесів і підвищення результативності. Правильно розроблена і реалізована ПолІБ дає змогу зменшити час недоступності сервісів, викликаних інцидентами ІБ, таким чином поліпшити показники живучості організації.

Демонстрація зацікавленості керівництва в забезпеченні інформаційної

безпеки значно підвищить пріоритет безпеки в очах працівників організації.

Створення корпоративної культури ІБ і широке залучення працівників в процес забезпечення інформаційної безпеки. Необхідно переконати працівників в тому, що забезпечення ІБ – їх прямий обов'язок. Це досягається шляхом введення процедури обов'язкового знайомства з вимогами ПолІБ і підписанням відповідного документа про те, що працівник з ними ознайомлений, вони йому зрозумілі і він зобов'язується їх виконувати. Політика інформаційної безпеки дає підстави ввести вимоги щодо підтримання необхідного рівня ІБ в перелік обов'язків кожного працівника. Також ПолІБ допомагає створити в організації атмосферу, сприятливу для пропаганди і підтримки високого пріоритету ІБ.

Зменшення вартості страхування. Наявність ПолІБ є необхідною і обов'язковою умовою укладання договорів страхування. Зауважимо, результати аудиту ІБ, проведеного незалежною організацією, впливають на вартість страхування.

Економічна доцільність. ПолІБ є дешевим і водночас доволі ефективним засобом забезпечення ІБ. Її послідовне втілення і чітке дотримання декларованих нею вимог у щоденному житті організації дозволяє знизити витратну частину бюджету, яка скеровується на забезпечення ІБ.

Успішна бізнес-практика. Наявність ПолІБ сприймається у бізнес-колах як вияв дотримання організацією правил хорошого тону.

Таким чином, політика інформаційної безпеки є вкрай необхідною для успішної організації режиму ІБ будь-якої вітчизняної організації. ПолІБ мінімізує вплив "людського фактора" і недоліки існуючих технологій захисту інформації. Крім того вона дисциплінує працівників організації і сприяє створенню корпоративної культури безпеки.

Література

1. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1985 [Electronic resource]. – Access mode : http://csrc.nist.gov/publications/history/dod85.pdf