УДК 65.012.8

ОБГРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ НА ПІДПРИЄМСТВАХ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Шиптицька І.І.

Кухарська Н.П., канд. фіз.-мат. наук, доцент

Львівський державний університет безпеки життєдіяльності

У системі управління безпекою життєдіяльності людини та суспільства все більшого значення набуває забезпечення інформаційної безпеки (ІБ) підприємства, що пов'язано із постійним стрімким зростанням обсягу інформації, з необхідністю її зберігання, передачі і обробки, з ускладненням архітектури сучасних інформаційних систем. Переведення значної частини інформації в електронну форму, зростання масштабів використання локальних і глобальних мереж породжують нові види загроз, вразливостей і ризиків, які мають безпосередній вплив на діяльність організації. У зв'язку з цим, сьогодні важливими завданнями керівництва кожного підприємства є запобігти загрозам інформації, мінімізувати ризики і забезпечити належний рівень безпеки IT-інфраструктури.

Інвестиції організацій в забезпечення інформаційної безпеки у вигляді залучення засобів технічного захисту інформації, витрат на оплату праці фахівців, на проведення зовнішнього аудиту безпеки і т.п., неухильно збільшуючись з року в рік, як правило, не окупаються. Відбувається це здебільшого тому, що більшість організацій продовжують дотримуватися фрагментарного підходу, який виправдовує себе тільки при слабкій залежності організації від інформаційних технологій і низькому рівні ризиків інформаційної безпеки. Адекватний стан інформаційної безпеки в змозі забезпечити тільки комплексний підхід, що передбачає планомірне використання як програмно-технічних, так і організаційних заходів захисту на єдиній концептуальній основі. Першочергову роль в системі організаційних заходів забезпечення інформаційної безпеки підприємства відіграє багаторівнева політика, основне завдання якої є відображати підхід організації до захисту інформаційних активів та ресурсів у відповідності до вимог бізнесу, партнерів, клієнтів, законодавчої бази.

Під терміном "політика інформаційної безпеки" (information security policy) розуміють сукупність документованих методологій і управлінських рішень, які регламентують порядок інформаційної діяльності в організації і спрямовані на захист інформації, інформаційних систем і асоційованих з ними ресурсів.

Розробка політики інформаційної безпеки – процедура аж ніяк не тривіальна, так як темпи розвитку сучасних інформаційних технологій значно випереджують темпи розроблення рекомендаційної та нормативно-правової бази, керівних документів, чинних на території України. Нещодавно (у 2010 році) Національний банк України запровадив [1] два галузеві стандарти управління

інформаційною безпекою [2, 3], які визначають вимоги і правила впровадження системи управління інформаційною безпекою та дублюють міжнародні стандарти ISO/IEC 27001 та ISO/IEC 27002. Залучення іноземних інвестицій в економіку України змушує вітчизні підприємства, на додачу до вимог і рекомендацій згаданих вище стандартів, Конституції України та інших керівних документів, дотримуватися також міжнародних рекомендацій. Так, українським підприємствам слід адаптувати до вітчизняних умов і застосовувати на практиці методики міжнародних стандартів, таких як ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL, а також методики управління інформаційними ризиками в поєднанні з оцінюванням економічної ефективності інвестицій підприємства в забезпечення захисту інформації.

Високорівнева політика інформаційної безпеки – це, як правило, доволі статичний документ, який містить:

- загальну інформацію про забезпечення ІБ в організації (в якій мотивовано визначено необхідність забезпечення і підтримки режиму безпеки);
- заяву про підтримку (commitment) заходів щодо забезпечення ІБ на всіх управлінських рівнях;
- основні положення стосовно визначення цілей ІБ;
- розподіл ролей і визначення загальної відповідальності за реалізацію заходів щодо забезпечення ІБ (у тому числі стосовно розробки і коригування політик);
- посилання на низькорівневі документи, які визначають порядок реалізації тих чи інших аспектів, пов’язаних з забезпеченням ІБ.

Крім висорівневої політики розробляють також низькорівневі політики (підполітики), які, зазвичай, відображають вимоги у певній області. Як приклад політики низького рівня можна навести політику управління доступом, політику управління паролями, політику резервного копіювання і т.п. Конкретний набір низькорівневих політик залежить від особливостей організації: її розміру, структури, корпоративної культури і т.п.

Документована політика ІБ повинна бути затверджена керівництвом і доведена до відома усіх працівників організації і зовнішніх сторін, до яких вона має відношення.

ЛІТЕРАТУРА

1. Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України; постанова правління Національного банку України від 28 жовтня 2010 р. № 474. – К. : Національний банк України, 2010.
2. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. – К. : Національний банк України, 2010. – 49 с.

3. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD). ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. – К. : Національний банк України, 2010. – 163 с.