МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

МЕНЕДЖМЕНТ І АДМІНІСТРУВАННЯ: ТЕНДЕНЦІЇ РОЗВИТКУ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ МАГІСТРІВ ТА МОЛОДИХ ВЧЕНИХ

ЗА ЗАГАЛЬНОЮ РЕДАКЦІЄЮ Л. О. ЗГАЛАТ-ЛОЗИНСЬКОЇ, М. І. ФІЛІПОВА

Київ
ДП «Видавничий дім «Персонал»
2011

ББК 65.290-2я43
М50

Рецензенти: *Г. А. Дмитренко* — зав. кафедри економіки і управління персоналом Університету менеджменту освіти Академії пед. наук України, д-р екон. наук, проф.
В. І. Пила — д-р екон. наук., проф.
Н. Д. Чала — доцент Академії муніципального упр., канд. екон. наук

Рекомендовано до друку Вченою радою Міжрегіональної Академії управління персоналом (протокол № 10 від 24.11.10)

Видання здійснене в рамках проекту "Наукові праці МАУП"

Менеджмент і адміністрування: тенденції розвитку: матеріали наук.-практ. конф. магістрів та молодих вчених, м. Київ, 23–24 верес. 2010 р. /за заг. ред. Л. О. Згалат-Лозинської, М. І. Філіпова. — К.: ДП «Видавничий дім «Персонал». — 272 с.: іл. — Бібліогр. в кінці ст.

М 50

Збірник "Матеріали науково-практичної конференції магістрів та молодих вчених "Менеджмент і адміністрування: тенденції розвитку" містить наукові статті, що стосуються актуальних питань розвитку менеджменту в Україні, зокрема менеджменту організацій, а також виробничих, готельно-туристичного комплексу, навчальних закладів, установ галузі охорони здоров'я, управління персоналом, інвестиційного та інноваційного менеджменту.

Для всіх, хто цікавиться розвитком менеджменту в Україні.

ББК 65.290-2я43

ЗМІСТ

УДК 618: 004.5

В. В. ВИСОЦЬКИЙ

докторант МАУП
начальник управління інформаційної безпеки ВАТ "Ітер Ком"

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ ПРИ ВИКОРИСТАННІ АУТСОРСИНГОВИХ ТЕХНОЛОГІЙ

Одним з важливих питань виведення IT-процесів на аутсорсинг є інформаційна безпека. Потрібно розуміти, що вся економічна ефективність аутсорсингу може бути втрачена, якщо станеться інцидент у частині інформаційної безпеки, в результаті якого компанія може зазнати збитків, які неможливо порівняти з отриманою від аутсорсингу економією. Збереження режиму інформаційної безпеки вимагає виконання певних вимог, які мають задовольняти як процеси забезпечення інформаційної безпеки, так й інші процеси IT-підрозділу. Одна з ключових вимог — налагоджена система по управлінню ризиками інформаційної безпеки з метою мінімізації їх наслідків або їх повному запобіганню, а також сформована технологічна інфраструктура, що забезпечує мінімізацію основних технологічних ризиків.

На сьогодні застосовуються дві моделі виведення IT-процесів на аутсорсинг: еволюційна та революційна. У рамках використання еволюційної моделі процеси і послуги виділяються послідовно, одна за одною, стороннім підрядчикам, при цьому співробітники IT-підрозділу залишаються у штаті компанії і поступово передають свої функції зовнішнім підрядчикам, концентруючись на завданнях вибору постачальників і контролю за результатами. Цей варіант дає можливість аналізувати всі процеси, що виводяться за межі організації, і здійснювати аналіз режиму інформаційної безпеки для кожного процесу, визначаючи ті заходи, які потрібно виконати для забезпечення необхідного рівня інформаційної безпеки.

При використанні революційної моделі IT-підрозділ організації разом зі своїми процесами виділяється в окрему юридичну особу і дістає можливість надання послуг як зовнішнім замовникам, так і самому підприємству. В цьому випадку необхідно включати нову юридичну особу в свою систему управління інформаційною безпекою і жорстко регламентувати питання обробки конфіденційної інформації аж до присутності фахівців з інформаційної безпеки у дочірній IT-компанії.

Одним з видів аутсорсингу є залучення в штат внутрішнього IT-підрозділу фахівців сторонньої IT-компанії. Таку послугу називають "аутстаффінг", і фактично це вироджений тип аутсорсингу, оскільки управлінням зовнішніми IT-спеціалістами займається сам замовник. Аутстаффінг застосовується в тих випадках, коли замовник тільки починає роботу із зовнішньою IT-компанією, не довіряючи їй, і тому на перших порах будує роботу із зовнішніми фахівцями під своїм керівництвом. Фактично при

такому варіанті взаємодії говорити про використання концепції аутсорсингу передчасно, проте питання інформаційної безпеки важливі і в цьому випадку. Для зовнішніх IT-спеціалістів необхідно ввести набір обмежень до доступу й організувати систему моніторингу над їх діями, що дає змогу звести до мінімуму просочування конфіденційної інформації.

До основних загроз безпеці інформації та нормального функціонування інформаційних систем відносять: витік конфіденційної інформації; компрометація інформації; несанкціоноване використання інформаційних ресурсів; помилковий обмін інформацією між абонентами; відмова від інформації; порушення інформаційного обслуговування; незаконне використання привілеїв.

Якщо замовник та виконавець працюють за міжнародними стандартами, то аутсорсингові процеси можуть бути і прозорими, і контрольованими, й економічно обґрунтованими. Якщо чітко розмежувати зони відповідальності, визначити завдання постачальника аутсорсингових послуг і закріпити це все в SLA (Service Layer Agreement), можна істотно мінімізувати виникнення загроз інформаційній безпеці. Єдиним аспектом, що непідвладний SLA й міжнародним стандартам, є "людський фактор".

Ризики від передачі контролю можна мінімізувати, наприклад, за рахунок розмежування доступу, зокрема, компанія-аутсорсер насамперед може взяти під свій контроль периметрові засоби захисту, при цьому клієнт має сконцентруватися вже безпосередньо на внутрішніх критичних ресурсах мережі. Такий підхід зменшить ризики від зовнішніх загроз, але при цьому практично не збільшує внутрішні ризики, наприклад, від витоків даних.

Також для мінімізації ризиків у згодах та договорах між замовником, який виводить IT-процеси на аутсорсинг, й виконавцем можуть регламентуватися такі питання: згода про рівень сервісу (SLA); згода про нерозголошення інформації (NDA); регламент доступу до потужностей та каналів зв'язку, що орендуються замовником; регламент інформування про спроби несанкціонованого доступу ззовні; порядок контролю замовником виконання зобов'язань виконавцем та ін.

Ключові показники ефективності, за якими можна простежити ефективність побудованої системи інформаційної безпеки, можуть бути інтегровані в систему управління ризиками та піддаватися регулярному моніторингу. На цій стадії здійснюється моніторинг заздалегідь встановлених заходів, що спрямовані на зменшення обсягу збитку або частоти появи ризиків. Результати такого процесу можуть використовуватися з метою аудиту для підготовки компанії до сертифікації за стандартом ISO/IEC 27001:2005 (Information technology — Security techniques — Information security management systems — Requirements).

У випадку аутсорсингу регламентація питань інформаційної безпеки несе обов'язковий характер, оскільки зони повноважень та відповідальності мають бути визначені заздалегідь, і у випадку інциденту треба чітко ідентифікувати відповідальних та визначити винних.