ЕКОНОМІКО-МАТЕМАТИЧНІ МОДЕЛІ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ

УДК 004.5

В. В. ВИСОЦЬКИЙ
ВАТ "Ітер Ком"

АУТСОРСИНГ ЯК ТЕХНОЛОГІЯ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

В статті розглядається передача управління інформаційними процесами та функціями на обслуговування іншому підприємству як спосіб зменшення ризиків, пов'язаних з різними видами загроз інформаційній безпеці, що викликані, зокрема, дефіцитом спеціалістів у сфері IT.

Transfer of information management processes and functions to the outsource of another organization as a way to reduce the risks associated with various types of information security threats caused by, inter alia, the lack of specialists in the IT Industry.

Ключові слова: аутсорсинг, інформаційна безпека, ризик.

Вступ. В даний момент Україна, як і більшість інших технічно розвинутих держав, зазнає дефіцит спеціалістів сфери інформаційних технологій. За даними дослідницької компанії IDC[7], число спеціалістів у сфері IT складає 14% зайнятого населення Північної Америки, при цьому потреба в IT-професіоналах продовжує зростати. За прогнозами компанії, дефіцит кадрів у цій області збережеться до 2012 року. Спеціалісти IDC відмічають найбільш гостру нестачу спеціалістів по бездротовому та голосовому зв'язку (потребу в таких спеціалістах зазнають, відповідно, 19% та 35% серед 500 опитуваних компаній). Більш того, в області мережевої безпеки до 2011 року вакантними залишаться 11% посад, а загальний дефіцит кадрів складає 35 тисяч чоловік. По даним аналітичної компанії IDC, у 2007 році нестача лише спеціалістів в області мережевих технологій у нашій країні складала більш ніж 23 тисяч чоловік. Згідно дослідженню, що проводила IDC за замовленням компанії Cisco[6], у 2008 році дефіцит кваліфікованих спеціалістів складав більш ніж 28 тисяч чоловік(33.5%). Виходячи з цього, велика ймовірність того, що рівень кваліфікації співробітників, що забезпечують інформаційну безпеку, буде недостатньо високим, а це може спричинити збільшення ймовірності втрати даних, несанкційованого їх використання та інше.

Види загроз безпеці інформації. За природою виникнення загрози можна поділити на два класи:

1) природні або об'єктивні;

2) штучні або суб'єктивні.

Природні загрози викликані стихійними природними явищами, які не залежать від людини (землетруси, повені, урагани та інше).

Штучні загрози викликані діяльністю людини. До них відносять:

– ненавмисні загрози, які викликані помилками в проектуванні, монтажі обладнання і його експлуатації;

– навмисні загрози, що пов'язані з певними прагненнями людей, такими як тероризм, страйки, розкрадання, крадіжки, підслуховування, несанкційований доступ до комп'ютерних мереж та інше

Загрози також можуть підрозділятися за положенням джерела загрози. Джерело загрози може бути розташоване:

– поза контрольованою зоною, наприклад, перехоплення даних, що передаються по каналам зв'язку;

– в межах контрольованої зони, наприклад, розкрадання інформації, її носіїв, знищення інформації;

– безпосередньо в системі, наприклад, некоректне використання ресурсів.

Навмисні загрози, в свою чергу, поділяються на активні й пасивні. Пасивні загрози направлені, в основному, на несанкційоване використання інформаційних ресурсів, при цьому не відбувається вплив на функціонування системи. Наприклад, несанкційований доступ до баз даних, прослуховування каналів зв'язку та інше.

Активні загрози мають на меті порушення нормального функціонування інформаційної системи шляхом цілеспрямованого впливу на її компоненти. До активних загроз відносять, наприклад, вивід з ладу комп'ютера чи його операційної системи, руйнування програмного забезпечення, порушення роботи ліній зв'язку і т.д. Джерелом активних загроз можуть бути дії зловмисників, шкідливі програми та інше.

До основних загроз безпеці інформації та нормального функціонування інформаційних систем відносять:

– витік конфіденційної інформації;

– компрометація інформації;

– несанкційоване використання інформаційних ресурсів;

– помилковий обмін інформацією між абонентами;

– відмова від інформації;

– порушення інформаційного обслуговування;

– незаконне використання привілей.

Враховуючи загальну недостачу спеціалістів, з чого випливає можливий високий рівень некомпетентності власних співробітників, можна сказати, що в цьому випадку підвищуються ризики, пов'язані зі всіма видами загроз безпеці. Для зменшення ймовірності виникнення цих різновидів ризиків має сенс передавати управління інформаційною безпекою на обслуговування іншому підприємству.

Причини передачі управління інформаційними ресурсами на аутсорсинг. В даний час в літературі виділяють три основні причини аутсорсингу [5]:

1. Відмова від непрофільних видів діяльності. Це означає припинення розвитку в підприємстві певних видів діяльності, які не являються ключовими для реалізації вибраних стратегій, а також для створення й утримання підприємством конкурентних переваг.

2. Необхідність підвищення якості обслуговування. Тут йде мова про те, що затрати на якість починають перевищувати додану кінцевим товарам й послугам цінність, за яку міг би заплатити споживач. При цьому відбувається пошук зовнішніх постачальників, що виконують аналогічну роботу за меншу вартість або за ту ж саму вартість, але більш високої якості (зазвичай основний акцент робиться саме на підвищення якості).

3. Фінансова. Ця причина виникає коли з'являється необхідність скоротити витрати, зокрема за рахунок скорочення співробітників, які займаються інформаційними технологіями.

Крім цього, можна додати ще одну причину — необхідність зменшення ймовірності виникнення загроз безпеці. В цьому випадку, побічно, може підвищуватися якість обслуговування, що стосується фінансової сторони, то витрати можуть як скоротитися, так і підвищитися, якщо це потребує підвищення безпеки, наприклад, для зменшення ризиків, пов'язаних з природними загрозами безпеці може з'явитися необхідність у географічному рознесенню сховищ даних та швидкісних лініях зв'язку між ними.

Форми IT-аутсорсингу. Існує три основні форми IT-аутсорсингу[2].

1. Ресурсний аутсорсинг (аутсорсинг персоналу). Застосовуючи цю форму аутсорсингу, компанія-замовник використовує аутсорсера, як компанію по підбору висококваліфікованого персоналу. При цьому замовник, використовуючи зовнішні ресурси, сам ними управляє і, відповідно, самостійно несе відповідальність за результат. Постачальник послуг, в свою чергу, повинен забезпечити замовника ресурсами потрібного рівня й своєчасно здійснити їх заміну, якщо це необхідно.

2. Функціональний аутсорсинг — аутсорсер повністю бере на себе всі функції, які замовник йому передає. Безумовно, критерії роботи аутсорсера, включаючи швидкість реакції на нештатну ситуацію, ступінь участі в нестандартних проблемах і т.д., заздалегідь обговорюються й закріплюються в спеціальній угоді. Завдяки функціональному аутсорсингу компанія може підвищити ефективність управління своїми витратами й значно підвищити якість IT сервісів.

3. Стратегічний аутсорсинг має на увазі повну передачу управління IT-службами компанії аутсорсеру.

Виходячи з вищевикладених форм, можна сказати, що ресурсний аутсорсинг практично не впливає на зміни ризиків для інформаційної безпеки; вплив функціонального аутсорсингу залежить від того, які саме функції передаються на обслуговування у стороннє підприємство, чи мають ці функції вплив на безпеку. При цьому стратегічний аутсорсинг дозволяє повністю перекласти управління ризиками на стороннє підприємство, та при наявності в цьому підприємстві відповідних ресурсів (компетентних співробітників тощо) різко знизити ризики виникнення загроз інформаційній безпеці.

При цьому, треба помітити, що, не зважаючи на повну передачу управління IT службами, необхідно тісне співробітництво між аутсорсером та керованою компанією, а також готовність зі сторони керівництва керованої компанії виконувати рекомендації аутсорсера.

Безпека аутсорсингу. Якщо замовник та виконавець працюють по міжнародним стандартам, то аутсорсингові процеси можуть бути й прозорими, й контрольованими, й економічно обґрунтованими. Якщо чітко розмежовувати зони відповідальності, визначивши задачі постачальника аутсорсингових послуг та закріпити це все в SLA (Service Layer Agreement), то можна суттєво мінімізувати виникнення загроз інформаційній безпеці. Єдиний аспект, непідвладний SLA та міжнародним стандартам, це "людський фактор".

Ризики від передачі контролю можна мінімізувати, наприклад, за рахунок розмежування доступу, зокрема, компанія-аутсорсер, в першу чергу, може взяти під свій контроль периметрові засоби захисту, при цьому клієнт сконцентрується вже безпосередньо на внутрішніх критичних ресурсах мережі. Такий підхід зменшує 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 наступні 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 несанкційованого доступу ззовні;

• порядок контролю замовником виконання зобов'язань виконавцем та інше.

Ключові показники ефективності, по яких можна прослідкувати ефективність побудованої системи інформаційної безпеки, можуть бути інтегровані в систему управління ризиками та піддаватися регулярному моніторингу. Крім того, на цій стадії виконується моніторинг заздалегідь встановлених заходів, що націлені на зменшення об'єму збитку чи частоти появи ризиків. Результати даного процесу можуть використовуватися з метою аудиту для підготовки компанії до сертифікації по стандарту ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements)[4].

У випадку аутсорсингу регламентація питань інформаційної безпеки несе обов'язковий характер, оскільки зони повноважень та відповідальності повинні бути визначені заздалегідь, і у випадку інциденту треба чітко ідентифікувати відповідальних та визначити винних. В даний час найбільш часто використовують такий механізм, як згода про нерозголошення інформації, але його виконання не завжди можна проконтролювати, особливо якщо до конфіденційної інформації має доступ безліч осіб. Тому для забезпечення режиму інформаційної безпеки необхідні ефективні системи як у постачальника, так і у підрядника [9].

Підсумок. Таким чином можна припустити, що при необхідності підвищення якості обслуговування, при впровадженні аутсорсингу будуть зменшуватися ризики, що пов'язані з природними та штучними причинами, але при цьому може збільшуватися ймовірність загроз, джерела яких розташовані всередині контрольованої зони, за рахунок доступу до цієї зони підприємства, що здійснює аутсорсинг.

У випадку превалювання фінансової складової, зміна ступеня ризику залежить від досвіду й знань, якими володіли звільнені співробітники ІТ в порівнянні з досвідом та знаннями співробітників, які працюють у підприємстві, що надає аутсорсинг. При інших рівних умовах, ступінь ризику буде збільшуватися за рахунок внутрішніх загроз.

Аутсорсинг за рахунок відмови від непрофільних видів діяльності несе в собі ті ж самі ризики, що й аутсорсинг з фінансових причин, але, при цьому, фінансова складова не має такого пріоритету, що дозволяє направити більше ресурсів на аутсорсинг та за рахунок цього зменшити зовнішні ризики.

Висновок. Виходячи з вище викладеного, видно, що для зменшення ризиків від різних загроз інформаційній безпеці, можлива передача управління інформаційними процесами та функціями на обслуговування іншому підприємству, при цьому ризики від втрат даних, що пов'язані з природними загрозами, некомпетентністю власних робітників, нестачею обладнання, несанкційованим втручанням, понижуються, залежно від форми аутсорсингу, хоча при цьому можуть виникати ризики, пов'язані з доступом до конфіденційних даних компанії зі сторони підприємства, що здійснює обслуговування.

Література

1. Sparrow E. Successful IT Outsourcing / Elizabeth Sparrow — Springer, 2003 — 288pp. - ISBN 1-85233-610-2

2. ИТ-аутсорсинг гайд [Електронний ресурс] : (портал Outsourcing). – 2010. – Режим доступу : http://www.outsourcing.ru/content/rus/rubr58/rubr-583.asp.

3. Embrechts P. Quantitative Risk Management: Concepts, Techniques, and Tools / Alexander J. McNeil, Rüdiger Frey,. Paul Embrechts - Princeton University Press — 2005 — 608pp.

4. Information technology - Security techniques - Information security management systems - Requirements: ISO 27001:2005 - [Чинний від 2008-10-15]: Міжнар. Стандарт. – 34р.

5. Хейвуд Дж. Б. Аутсорсинг. В поисках конкурентных преимуществ / Хейвуд Дж. Б. – Вильямс, 2002. – 176 с.

6. Дефицит специалистов по сетевым и телекоммуникационным технологиям к 2008 году может стать критическим[Електроний ресурс] : (Cisco Systems, Inc.). – 2005. – Режим доступу : http://www.cisco.com/web/RU/news/releases/txt/0443.html.

7. IDC Ukraine [Електроний ресурс]. – Режим доступу : http://www.idcukraine.com

8. Quantifying the Business Impact Analysis: A New Model [Електронний ресурс]. – Режим доступу : http://www.miora.com/articles/gcc.htm

9. Беркович В. Вопросы информационной безопасности при аутсорсинге IT-процессов компании / В. Беркович, А. Коптелов [Електронний ресурс]. – 15.05.2007. – Режим доступу : http://citcity.ru/15815/

Надійшла 14.03.2010