УДК 330.3

О.І. Кір'ян

Українська інженерно-педагогічна академія, Харків

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕКОНОМІЧНОЇ ІНФОРМАЦІЇ ПРИ ВПРОВАДЖЕННІ НА ПІДПРИЄМСТВІ БІЗНЕС-ІНЖИНІРИНГУ

У сучасних умовах господарювання все більше підприємств та організацій впроваджують в практичну діяльність один з елементів світової практики управління – бізнес-інжиніринг. Окремі його елементи використовувалися ними з самого початку користування комп'ютерами в управлінні. Тобто, при значній механізації управлінських процесів процес впровадження елементів бізнес-інжинірингу ставав майже автоматичним. Значна кількість управлінських операцій стала виконуватися за допомогою персонального комп'ютеру. При цьому більшість організацій самотужки або з використанням спеціалістів впровадила переміщення окремих документів та функцій з комп'ютера на комп'ютер в сітці підприємства. Ті ж організації, що мали філії, заділи Інтернет, за допомогою якого документообіг прискорився.

Це, з одного боку, спростило роботу управлінського персоналу, зробило її більш творчою, дало можливість отримувати одночасно більшу кількість інформації для прийняття управлінського рішення; та з другого – зробило доступною майже всю інформацію підприємства або організації для будь-кого, хто має доступ до хоч якогось персонального комп'ютеру підприємства та має мінімальні навички щодо користування ним. Тобто, інформація підприємств та організацій стала майже незахищеною від конкурентів та недоброзичливих громадян.

Як показала практика, більшість користувачів організації переймаються лише тим, щоб до їх комп'ютерів не потрапили віруси. Тому майже всі використовують постійно оновлюванні антивірусні програми. Та є ще багато моментів .які повинні, на мій погляд, ураховуватись при роботі. Та застосовуватись майже у формі суворих наказів до виконання.

Першою проблемою є лінощі щодо збереження інформації на носіях. Окремих від комп'ютера користувача. Коли він сам втрачає частку або всю інформацію. Це особиста проблема, що спричиняє труднощі йому та безпосередньо колегам. Але в інших зберігається більша частка отриманої від нього інформації, і тому поновити її не досить важко. Коли ж на підприємстві впроваджено систему бізнес-інжинірингу, майже вся система керування ним не потребує дублювання інформації, і тому втрата будь-якої частки формує значні проблеми як для самого працівника, так і для всього колективу. Тому першим правилом безпеки є чітко розроблений, впроваджений та постійно контролюємий механізм зберігання інформації. До цього, на жаль, частіш звертаються керівники та бухгалтери фірм, ніж працівники великих організацій, та й ті лише після практики втрати інформації.

Другим кроком є, на погляд автору чітке відокремлення інформаційних блоків кожного працівника чи відділу. Які повинні бути задіяні в загальній системі бізнес-інжинірингу, та ті, що призначені для особистої поточної роботи. Це краще за все проілюструвати на прикладі конструкторського бюро. У нью-

му є інформація про всі розробки, що впроваджуються на підприємстві, тобто й нові технологічні процеси, що досить часто цікавлять конкурентів. Тому при стандартному підході до зберігання інформації кожен, хто отримав доступ до сітки підприємства або організації, може оглянути всю їх інформаційну базу. Більшість працівників каже, що не може поділити інформацію – для цього потрібно використовувати дуже складні програми. Але всі знають, як можна поділити комп'ютер між кількома користувачами, застосовуючи пароль, щоб інший не міг зайти в окремі документи. Тобто, для кількох людей це застосувати можливо. Значить, це можливо використовувати й для різних інформаційних блоків. Звичайно, від якісного хакера це не врятує, але ускладнить справу для недоброзичливого користувача. Тобто, керівництву підприємств та організацій також необхідно при впроваджені бізнес-інжинірингу пояснити як кожному працівнику, так і розробнику системи необхідність такого розподілу та кодового захисту інформації та без нього не дозволяти під'єднувати комп'ютер до мережі організації.

Третя складова стосується розробників системи бізнес-інжинірингу для організації. Саме вони повинні виконати вимоги керівництва, і загальну інформацію також розбити на блоки, що до них мають доступ керівники та користувачі різних рівнів. Це ускладнює та уповільнює впровадження завдання, але забезпечує зберігання комерційної таємниці на кожному рівні. Тому керівництву потрібно бути дуже уважними при формуванні завдання щодо впровадження бізнес-інжинірингу, та наполегливими й досить прискіпливими при його прийомі.

Також слід звернути увагу на такий елементарний прийом як «захист від дурня». Це досить рідко використовують на практиці великі підприємства, та значно частіше – маленькі фірми, що вже стикалися з проблемою помилкового знищення інформації. Тому важливо використовувати декілька запобіжних заходів. Це, по-перше, формування постійного запиту щодо необхідності видалення документів, тобто вимога від користувача підтвердження бажання знищити інформацію. По-друге, чітке визначення права видаляти. коректувати або лише використовувати інформацію для роботи.

Наведені прийоми на перший погляд усім знайомі, не мають особливої новизни. Але при практичній роботі завдяки цим якостям про них просто забувають, тим самим ставлячи під загрозу використання найякісніших програм, найкращого впровадженого бізнес-інжинірингу. Це ті «маленькі гвинтики», без яких неможлива постійна якісна робота автоматизованих систем управління підприємствами та організаціями.

Список літератури

1. Железко Б.А. Теория и практика построения информационно-аналитических систем поддержки принятия решений / Б.А. Железко, А.Н. Морозевич. – Мн.: Армита – Маркетинг, менеджмент, 1999. – 346 с.

2. Щенников С.Ю. Реинжиниринг бизнес-процессов. Экспертное моделирование, управление, планирование и оценка / С.Ю. Щенников. – М.: Ось-89, 2004. – 288 с.