Секція 2

Гаркуша С.А.
к.е.н., доцент кафедри бухгалтерського обліку
Сумський національний аграрний університет

ЗАХИСТ БУХГАЛТЕРСЬКОЇ ІНФОРМАЦІЇ: ТЕХНІЧНІ АСПЕКТИ

У процесі роботи в інформаційну базу щодня вводяться первинні дані: створюються нові документи, елементи довідників та ін. Розмір інформаційної бази при цьому поступово збільшується.

Разом з іншими даними може бути втрачена і робоча база. Наслідки повної втрати даних (при відсутності резервних копій на інших комп'ютерах / компакт-дисках і ін знімних носіях) дуже складно переоцінити. Не існує вічного обладнання; рано чи пізно з ладу вийде навіть найдорожчий і стабільний комп'ютер.

Співробітники підприємств, які не мають штатного системного адміністратора, іноді навіть не замислюються про збереження даних. Наслідки подібної безпечності можуть бути найсумніші.

Проблема захисту інформації при використанні мережевих продуктів без паперового обліку, якими користуються велика кількість користувачів, постає надзвичайно гостро. Сформовані в системі бази даних при відсутності адекватних заходів можуть бути видалені з необережності, зламані або передані зацікавленим особам.

Особлива увага повинна бути приділена захисту даних, що містяться в обліковій системі. На жаль, внутрішньої системи захисту даних недостатньо для запобігання всіх ризиків із витоку конфіденційної інформації. Це й копіювання даних, й крадіжка або несанкціоноване вилучення серверного обладнання,

арешт майна, дії конкурентів, спрямовані на зупинку роботи підприємства, рейдерське захоплення та ін.

Потрібно застосовувати надійні системи криптозахисту інформації для мінімізації ризиків на всіх етапах операцій з даними, починаючи з простих моделей файл-серверних побудов роботи, і закінчуючи розподіленими серверними рішеннями, включаючи весь ланцюжок резервування бази.

Варто застосовувати концепцію захисту даних побудовану на використанні апаратно-програмного комплексу, яка повинна надавати такі можливості:

- обмеження доступу до конфіденційної інформації шляхом надійного шифрування даних;
- висока швидкодія завдяки використанню алгоритмів шифрування, вбудованих в центральний процесор;
- надання доступу до захищених даних тільки після двофакторної аутентифікації;
- виключення ризику несанкціонованого копіювання баз даних навіть користувачами з правами адміністратора;
- підтримка всіх дискових систем, що використовуються на сервері (DAS, SAN, RAID);
- миттєва повна заборона доступу до захищених даних у випадку надзвичайних ситуацій;
- простота і зручність у використанні.

Інший спосіб захисту даних – захистити комп'ютер та програму від несанкціонованого доступу третіх осіб:

- поставити паролі, починаючи від входу в Windows і закінчуючи запуском бази;
- не залишати відкритою програму, коли працівник йде у справах з офісу;
- в деяких програмах існують засоби розмежування доступу, наприклад, можна заборонити користувачам переглядати певні документи, журнали документів,

довідники або звіти, користуватися певними обробками, знову ж для безпеки даних, тобто користувач повинен мати доступ тільки до тієї інформації , яка йому необхідна для роботи;

- не потрібно і забувати про обережність – часто офісні працівники мають доступ до Інтернету, а подорожуючи по непов'язаним з роботою сайтам легко «підчепити» троянську програму або вірус, як наслідок – збій в системі та можлива втрата даних;
- і зовсім вже зайве писати паролі для входу в базу на листочках, приклеєних до монітора або біля робочого столу, залишати, де попало смарт-карти та інші засоби ідентифікації, а якщо за комп'ютером працює інша людина, краще простежити за інформацією, яку він переглядає.

Забезпечення безпеки інформації – дорога справа, і не тільки через витрати на закупівлю або установку засобів захисту, але також через те, що важко кваліфіковано визначити межі розумної безпеки і забезпечити відповідне підтримання системи в працездатному стані.

Література

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL : http://zakon5.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

2. Захист інформації. Технічний захист інформації. Терміни та визначення (ДСТУ 3396.2-97), [Чинний від 1998. 01-01]. Вид. офіц. Київ : Державна служба спеціального зв'язку та захисту інформації України. URL : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38934&cat_id=38836