УДК 004.052.2:004.056

Кухарська Н. П.
кандидат фізико-математичних наук, доцент
Львівський державний університет безпеки життєдіяльності
Лагун А. Е.
кандидат технічних наук, доцент
Львівський державний університет безпеки життєдіяльності

ІНФОРМАЦІЙНА БЕЗПЕКА ПРОЦЕСУ УПРАВЛІННЯ БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ

У зв’язку з залежністю як бізнесу, так і державних структур від якості та цілісності інформації, використовуваних автоматизованих інформаційних систем, грамотна організація захисту інформаційних активів набуває дедалі більш важливого значення. У сучасному суспільстві нарешті прийшли до розуміння того, що задоволення вимог стандартів з питань управління інформаційною безпекою не можна розглядати як разову акцію. Насправді, це безперервний процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою.

Донедавна (до появи у квітні 2012 року міжнародного стандарту ISO/IEC 27031:2011 [1]) управління інформаційною безпекою розглядалося відірвано від управління безперервністю бізнесу. Щоправда, одним із перших винятків був стандарт України з інформаційної безпеки в банківській сфері [2], цілий розділ (розділ 14) якого присвячений взаємозв'язку інформаційної безпеки з управлінням безперервністю бізнесу.

Управління безперервністю бізнесу (Business Continuity Management, BCM) — це цілісний процес управління, в рамках якого ідентифікуються потенційні загрози діяльності організації, оцінюється їх можливий вплив на бізнес-операції, а також створюється основа для забезпечення здатності

організації відновлювати свою діяльність і ефективно реагувати на інциденти, що гарантує дотримання інтересів зацікавлених сторін, забезпечує захист репутації, бренду і операцій, що мають цінність [1].

Основною метою корпоративних програм управління безперервністю діяльності є мінімізація ризику втрати бізнесу в разі його переривання, а також продовження діяльності компанії в умовах надзвичайної ситуації. Ефективність системи управління безперервністю бізнесу часто залежить від готовності інформаційних технологій (IT) гарантувати, що цілі організації продовжуватимуть досягатися і у випадку серйозних аварій інформаційних систем, спричинених, наприклад, природними лихами, нещасними випадками, відмовами обладнання, а також навмисними діями людей.

Готовність IT до забезпечення безперервності бізнесу (ICT Readiness for Business Continuity, IRBC) – це важлива (поряд з політиками, процедурами і людьми) складова частина впровадження та функціонування системи управління безперервністю бізнесу. Щоб забезпечити цю готовність організації мають втілювати в життя низку рішень з арсеналу катастрофостійких технологій. За своєю суттю ці технології передбачають резервування ресурсів інформаційної системи та резервне зберігання даних.

Розглянемо більш детально технології резервування даних, так як у разі надзвичайних ситуацій найбільші збитки організації завдаються не тимчасовою неможливістю доступу до критичних даних, а цілковитою їх втратою. У статті [3] подано класифікацію методів резервування даних інформаційних систем, автори якої окремо виділяють методи резервного копіювання та реплікації даних.

Резервне копіювання (backup) – процес створення копії даних на носієві (жорсткому диску, флеш-пам’яті і т.д.) задля подальшого відновлення цих даних в оригінальному місці їх розташування в разі їхнього пошкодження або руйнування.

Резервне копіювання здійснюється програмним забезпеченням, яке на основі аналізу стану відповідного атрибуту файлу (біту архівування – archive

bit) приймає рішення чи потрібно включати цей файл у резервну копію, чи ні. Значення біту архівування встановлюють файлові системи операційних систем, які відслідковують зміни файлів. Якщо був створений новий файл чи модифікований існуючий, файлова система встановлює для цього файлу біт архівування в 1.

Резервне копіювання може бути повним, диференціальним чи інкрементним. Першим кроком на шляху до забезпечення готовності ІТ є створення повної резервної копії (full backup), тобто копії усіх даних на деякому зовнішньому носієві. У процесі створення такої копії біт архівування занулюється.

Більшість компаній на практиці використовує комбінацію повного резервного копіювання з диференціальним або інкрементним резервним копіюванням. Під час створення диференціальної резервної копії (differential backup) копіюються тільки новоутворені файли і ті файли, до котрих були внесені зміни з часу останнього повного копіювання. За необхідності відновлення даних, спочатку відновлюються дані з повної резервної копії, а потім поверх неї записуються дані із останньої диференціальної резервної копії. При створенні диференціальної копії значення біту архівування не змінюється.

У випадку створення інкрементної резервної копії (incremental backup) копіюються тільки ті файли, котрі були змінені з моменту останнього створення повної чи інкрементної резервної копії. У процесі побудови інкрементної копії біт архівування скидається (встановлюється в 0). За необхідності відновлення даних, спочатку проводиться відновлення файлів з повної резервної копії, а потім у правильному порядку поверх них записуються файли кожної наступної інкрементної резервної копії.

Який варіант резервного копіювання є найкращим? Організація може прийняти рішення використовувати лише повне резервне копіювання, якщо її приваблює відновлення даних в одну дію. Однак у цьому випадку процедура створення резервних копій вимагатиме затрат доволі великої кількості часу. Використання диференціального чи інкрементного резервного копіювання є

більш складним. Позаяк, такі стратегії потребують значно менше ресурсів і часу. Диференціальне резервне копіювання, в порівнянні з інкрементним, вимагає більше часу на створення резервних копій і, водночас, менше часу на етапі відновлення даних, котрий, у свою чергу, завжди ділиться лише на два підетапи (відновлення повної копії і відновлення диференціальної копії). Інкрементне резервне копіювання забирає менше часу при створенні резервних копій (оскільки копіюється менший об'єм інформації), але для відновлення даних потребує його більше через необхідність відновлення інформації з декількох інкрементних копій.

Зауважимо, яка б стратегія резервного копіювання не була обрана організацією, вона повинна враховувати ймовірність появи проблеми на будь-якому кроці процесу створення резервної копії чи відновлення файлів з неї. Спеціально, на випадок непередбачуваного пошкодження даних, в стратегії повинна бути закладена можливість "відкоту" здійснених змін чи реконструкції даних на самий початок.

Література

1. Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity : ISO/IEC 27031:2011 [Electronic resource]. – Access of mode : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374.

2. 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.

3. Пархуць Л. Організаційно-технічне забезпечення процесу відновлення інформаційно-комунікаційних систем після аварії / Л. Пархуць, Т. Хома, О. Хмиз // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012. – Вип.1. – С. 76–83.