УДК 681.3.07

В.М. Бурлаков, О.О. Кернасовська

МОДЕЛЬ ГАРМОНІЗОВАНОГО СТАНДАРТУ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ УПРАВЛІННЯ РЕСУРСАМИ ПІДПРИЄМСТВА

Враховуючи комплексну природу систем управління ресурсами підприємства (Enterprise Resource Planning, ERP), найбільш актуальними проблемами при впровадженні ERP-рішень є не лише узгодження їх з існуючими на підприємстві бізнес-процесами або модифікація цих процесів з метою найбільш продуктивного використання можливостей таких систем, а й не менш гостре питання — безпека інформації. Адже система, яка здатна контролювати велику кількість організаційно-виробничих процесів підприємства, одночасно з перевагами може нести в собі і потенційну небезпеку, пов'язану, зокрема з несанкціонованими маніпуляціями, невірним відображенням даних, як виробничого так і фінансового характеру, шахрайством тощо.

I. Постановка задачі

Завдяки комплексності та високому ступеню інтеграції ERP-систем з бізнес-процесами підприємства, стає необхідним здійснення комплексного аналізу можливих ризиків з точки зору безпеки, і, як наслідок, фінансових ризиків, які є прямим наслідком впровадження системи класу ERP. При цьому варто зазначити, що доцільним є розгляд не лише безпеки на рівні функціонування і використання самої системи, а й опосередкованих ризиків, таких як:

- невірне відображення існуючих бізнес-процесів;
- неперенесення критичних механізмів контролю, які існували на рівні неавтоматизованих процесів, у ERP-систему (з їх модифікацією відповідно до нових потреб та методів реалізації);
- відсутність чітких та авторизованих повноважень співробітників-користувачів системи і, як наслідок, відсутність адекватного розподілу обов'язків;
- проблеми пов'язані з конвертацією даних з системи, що використовувалася раніше, їх неповне, некоректне або й взагалі невірне перенесення в нову систему.

При цьому не втрачають актуальність і більш загальні питання безпеки:

- відсутність на підприємстві офіційної політики у сфері інформаційної безпеки;
- відсутність відповідної інфраструктури інформаційної безпеки, методів та засобів контролю за порушеннями цієї політики,

 ISSN 1562-9945

- відсутність засобів забезпечення неперервності функціонування бізнесу та прорублених, чітко спланованих на всіх рівнях заходів відновлення функціонування систем і підприємства в цілому у разі надзвичайних ситуацій.

При цьому варто розглядати кожен з зазначених аспектів відповідно від типів архітектури ERP-системи: дворівневої або трирівневої. Дворівнева архітектура реалізується за допомогою центру обробки даних, який включає в себе сервер, орієнтований для обробки даних, та ПК користувача, який виступає у якості клієнта. Трирівнева архітектура передбачає існування також середнього ярусу, який виступає в якості проміжного логічного рівня між веб-клієнтом та базою даних. Схематичне зображення варіантів реалізації систем з точки зору архітектури наведено на рис. 1.

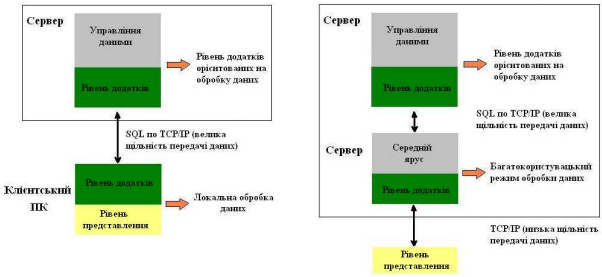

Рис. 1 – Архітектура ERP- систем

Окремим пунктом при аналізі зазначеного вище переліку постає питання безпеки на кожному з рівнів інфраструктури і, відповідно, архітектури:

- на рівні фізичної безпеки середовища, що передбачає обмежений доступ до систем та засобів зв’язку, усунення небезпеки несанкціонованого доступу до приміщень, систем та засобів;
- на рівні мережі, що передбачає застосування засобів і технологій, які здатні зашкодити доступу до мережі підприємства як на рівні віддалених атак, так і з середини;
- на рівні операційної системи: розподіл повноважень та рівнів доступу користувачів;
- на рівні системи управління базами даних (СУБД), що є критичною при роботі з конфіденційною бізнес-інформацією;
- на рівні базису ERP-системи, який виступає в ролі інтерфейсу між СУБД та безпосередньо ERP-системою, а отже здатен, при неправильному умисному чи неумисному налаштуванні, завдати значної шкоди системі;
- безпека самої ERP-системи, що включає як безпеку на рівні доступу, так і правильність налаштування і використання.

II. Загальні вимоги до безпеки корпоративних систем та мереж

Однією із запорук успіху при зменшенні ризиків, пов'язаних з безпекою ERP-систем є наявність стандарту у сфері інформаційної безпеки, здатного надати комплексну методологію та вимоги щодо забезпечення безпеки інформаційних систем та інформаційних активів.

Аналіз показує, що ті нормативні документи, які на сьогодні існують в Україні, є фрагментарними або вузькоспеціалізованими (такі як, наприклад, Постанови Національного банку України та нормативні документи Державної служби спеціального зв'язку та захисту інформації України) і не пристосованими для використання промисловими підприємствами, а тим більше не призначені для застосування в якості вимог по забезпеченню інформаційної безпеки при створенні комплексних систем управління ресурсами підприємств. Відтак, поставлена потреба аналізу вимог та розробки гармонізованого стандарту захисту інформації, придатного для використання в системах управління ресурсами підприємств.

Аналіз сучасних ERP–систем (на прикладі великих промислових систем Oracle E-Business suite та SAP R/3) показав, що ці системи зберігають та обробляють значну кількість конфіденційної інформації, яка може становити комерційну таємницю (наприклад, фінансові показники підприємства) чи персональні дані (наприклад, демографічну інформацію, дані щодо банківських рахунків фізичних осіб), захист якої є необхідним як для функціонування самого підприємства, так і для безпеки його клієнтів, партнерів та співробітників. Розглянемо, які загальні вимоги щодо безпеки корпоративних систем та мереж можуть бути використані для зазначених вище систем та інформації.

Основою концепцію, яка присутня в усіх світових стандартах у сфері захисту інформації, є концепція так званих механізмів контролю. Під цим поняттям мається на увазі система механізмів, правил та заходів призначених для здійснення контролю над різними сферами функціонування систем та бізнес-процесів, а також для попередження та виявлення можливих порушень в роботі окремих систем зокрема та процесів в цілому. Взагалі, IT-залежні процедури контролю можна поділити на дві основні категорії:

- загальні процедури контролю IT;
- прикладні системи контролю (контроль бізнес-процесів).

До першої групи відносяться всі ті механізми контролю, які безпосередньо пов'язані з IT як на рівні інфраструктури, так і на рівні адміністрування. Обидві ці категорії прийнято зображати за допомогою піраміди механізмів контролю, яка наочно зображає взаємозв'язок процедур контролю (рис. 2).

Другою узагальнюючою концепцією організації механізмів контролю, запропонованою Комітетом Організацій-Спонсорів комісії Тредуея (COSO – Committee of Sponsoring Organizations), є п'ятирівнева об'ємна модель,

 ISSN 1562-9945

Рис. 2 – Взаємозв’язок процедур контролю

представлена у вигляді кубу, звідки вона і дістала свою назву “COSO Куб” (рис. 3).

Рис. 3 – Куб COSO

Модель COSO була взята за основу при створені багатьох стандартів у сфері інформаційних технологій в цілому та захисту корпоративних систем та мереж зокрема. Завдяки своїй всеохоплюваності “COSO Куб” представляє собою скоріше спрямовуючі принципи, ніж керівництво до дії. Модель складається з п’яти ієрархічних рівнів:

- середовища контролю;
- оцінки ризиків;
- механізмів контролю;
- корпоративних комунікацій;
- моніторингу.

На основі цих вимог була розроблена більшість сучасних світових стандартів в сфері захисту інформації: CobIT, ISO/IES 17799:2005, ITIL, TOGAF, PMBOK, Prince2.

III. Гармонізація стандартів захисту інформації CobIT 4.1 та ISO/IEC FDIS 17799:2005 на базі експертної інформації

Для розробки моделі стандарту захисту інформації в системах управління ресурсами підприємств найбільш доцільно взяти всесвітньо визнані стандарти в царині захисту інформації: CobIT 4.1 та ISO/IEC FDIS 17799:2005. Але аналіз архітектури, змісту та основних положень чотирьох доменів CobIT та одинадцяти розділів ISO/IEC показує, що вони мають загальний характер, відтак постає питання можливості їх застосування для забезпечення інформаційної безпеки саме ERP-систем.

Для дослідження та розробки гармонізованого стандарту необхідно обрати доцільний математичний апарат, який би дозволив вирішити багатокритеріальну задачу оцінки важливості та доцільності критеріїв стандартів, які було взято за основу гармонізованого стандарту. Оскільки системи захисту інформації (СЗІ), з одного боку, є складовою частиною інформаційної системи, з іншої сторони самі по собі представляють складну технічну систему. Рішення задач аналізу й синтезу СЗІ ускладнюється деякими їх особливостями, основними з яких є:

- складний опосередкований взаємозв'язок показників якості СЗІ з показниками якості інформаційної системи;
- необхідність врахування великої кількості показників (вимог) СЗІ при оцінці й виборі їхнього раціонального варіанта;
- переважно якісний характер показників (вимог), що враховують при аналізі й синтезі СЗІ;
- істотний взаємозв'язок і взаємозалежність цих показників (вимог), що мають суперечливий характер;
- труднощі в одержанні вихідних даних, необхідних для вирішення задач аналізу й синтезу СЗІ, особливо на ранніх етапах їхнього проектування.

Зазначені особливості роблять практично неможливим застосування традиційних математичних методів, у тому числі методів математичної статистики й теорії імовірності, а також класичних методів оптимізації для рішення прикладних задач аналізу й синтезу СЗІ.

Складність процесу прийняття рішень, відсутність математичного апарата призводять до того, що при оцінці й виборі альтернатив можливо, а найчастіше просто необхідно, використати й обробляти якісну експертну інформацію.

Таким чином, для проведення оцінки вимог стандартів необхідно розробити модель матриць оцінювання систем інформаційної безпеки ERP-систем, яка дозволить шляхом використання експертних оцінок, з одного боку, визначити найважливіші компоненти стандартів, а з іншого боку – ті з них, що найбільш релевантні до сучасних ERP-систем. При

 ISSN 1562-9945

цьому виникає задача визначення важливості (ваги) вимог, що висуваються до параметрів СЗІ. Оскільки при вирішенні задачі перед нами, практично, стоїть задача багатокритеріального порівняння та оцінки стандартів, то доцільним буде скористатися методом власних векторів Уея [1], який ґрунтується на даних матриці попарних порівнянь $A^+ = ||a_{ij}^+||, a_{ij} \in \{-1, 0, 1\}$, де $a_{ij} = -1$ означає перевагу параметра x_j над параметром x_i, $a_{ij} = 0$– рівноцінність x_j й x_i , $a_{ij} = 1$- перевагу параметра x_i над параметром x_j. Але через незручність роботи з негативними числами матрицю попарних порівнянь можна перетворити в ненегативну матрицю $A^+ = ||a_{ij}^+||, a_{ij} \in \{0, 1, 2\}$, де числа (0,1,2) мають вищезазначений зміст. Склавши числа по кожному з рядків матриці, будемо мати числові характеристики важливості параметрів, а розділивши їх на загальну суму - одержимо вагові коефіцієнти параметрів [1]:

$$\lambda_{ii} = \frac{\sum\limits_{j=1}^{n} a_{ij}^+}{\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{n} a_{ij}^+} \qquad \text{(III-1)}$$

Недоліком цієї формули є те, що вона не враховує важливість “нічийних” (рівноцінності x_jй x_i) і “програшних” (коли x_j перевершує x_i) порівнянь. Якщо усунути цей недолік, то ваговими коефіцієнтами по суті є координати власного вектора, що відповідає максимальному характеристичному числу матриці попарних порівнянь. При цьому очевидною є необхідність вирішення задачі багатокритеріальної оптимізації [2], що має наступний вигляд: нехай $X = |x_1, \ldots, x_i, \ldots, x_n|$ – вектор параметрів, що оптимізуються, деякої системи S. Деяка j-та властивість системи S характеризується величиною j-го показника $q_i(X)$, $j = [1, ..., m]$. Тоді система в цілому характеризується вектором показників $Q = |q_1, \ldots, q_j, \ldots, q_m|$. Задача багатокритеріальної оптимізації зводиться до того, щоб із множини M_s варіантів системи S вибрати такий варіант (систему S_0), що має найкраще значення вектора Q. При цьому передбачається, що поняття “найкращий вектор Q” попередньо сформульовано математично, тобто обраний (обґрунтований) відповідний критерій переваги (відношення переваги). Для вирішення нашої конкретної задачі найбільш прийнятним є метод адитивного показника. Адитивний показник якості являє собою суму зважених нормованих часткових показників і має вигляд:

$$Q = \sum_{j=1}^{m} \omega_j \bar{q}_j, \qquad \text{(III-2)}$$

де q_j – нормоване значення j-го показника, ω_j – ваговий коефіцієнт j-го показника, що має тим більшу величину, чим більше він впливає на якість системи:

$$\sum_{j=1}^{m} \omega_j = 1; \omega_j > 0; j = 1, m \qquad \text{(III-3)}$$

Варто зазначити, що методи, які використовуються для визначення вагових коефіцієнтів у формулі (III-2) були розглянуті вище.

У нашому випадку експертам було запропоновано оцінити вимоги за бінарним критерієм: "0" – критерій не релевантний захисту інформації в ERP-системах, "1" – критерій релевантний захисту інформації в ERP-системах. Таким чином для оцінки отриманих результатів було вирішено використати модифікований метод Уея, що має не три, а два значення матриці A: 0 або 1. При цьому для інтегральної оцінки використаємо адитивний критерій, застосовуючи його до кожного з параметрів, вважаючи, що всі експерти мають однаковий авторитет, а всі параметри – однакову вагу, тобто $\omega_j = 1$ для всіх q_j. В якості критичного значення задамо підтримку критерію не менш ніж шістьма експертами. Критерії, з кількістю балів нижче граничного рівня виключаються з подальшого розгляду.

Для подальшої оцінки відібраних для розгляду критеріїв існує два підходи: визначення рівня кваліфікації експертів, що проводять оцінювання, за умови рівнозначності параметрів, чи визначення важливості (ваги, значущості) окремих параметрів за умови, що оцінки експертів рівнозначні. В нашому випадку зручніше скористатися другим припущенням, оскільки експерти, що приймають участь в опитуванні мають приблизно однакову кваліфікацію і досвід роботи в сфері IT, а отже ступінь довіри до їх оцінок є близькою. Експертам було запропоновано зазначити важливість критеріїв, розподіливши між ними 100% загальних балів. Тоді згідно (III-3) виконується вимога рівності одиниці суми ваги, що надається кожним окремим експертом. Далі, скориставшись формулою (III-2) знаходимо сумарну важливість кожного критерію, нормовану згідно кількості експертів. Для даної задачі оцінювання, з метою досягнення найвищого ступеню об'єктивності та вилучення екстремальних значень, формулу (III-2) було модифіковано наступним чином:

$$q_j = \sum_{i=1}^{n} q_i - \min_i(q_i) - \max_i(q_i) \tag{III-4}$$

$$\omega_j = \frac{\sum\limits_{i=1}^{n} q_i - \min_i(q_i) - \max_i(q_i)}{\sum\limits_{j=1}^{m} q_j}, \tag{III-5}$$

де q_i – сумарна оцінка j-го критерію всіма експертами, за виключенням найбільшої та найменшої оцінки, поставленої даному критерію будь-ким з експертів; ω_j – вага j-го критерію нормована за модифікованою сумарною оцінкою усіх критеріїв.

Загалом механізм визначення та відбору необхідних критеріїв можна описати наступним чином:

- на базі розробленої моделі проводиться експертна оцінка релевантності вимог стандартів в розрізі їх застосування для систем управління ресурсами підприємств, а також оцінка того, які з вимог є крити-

чними для забезпечення безпеки, а отже визначається вага кожного критерію, відповідно до його важливості;

- ґрунтуючись на отриманих результатах з загального переліку представлених до розгляду вимог, відбираються ті, які могли б бути застосовані в ERP-системах;
- аналізується міра, з якою відібрані вимоги можуть бути реалізовані в сучасних промислових ERP-системах (на прикладі SAP R/3 та Oracle e-Business Suite) та визначаються критерії для створення моделі гармонізованого стандарту, базуючись на їх важливості та не однаковому рівні реалізації в досліджуваних системах.

Кінцевим результатом проведеного дослідження є розробка моделі гармонізованого стандарту захисту інформації в системах управління ресурсами підприємств, який враховує специфіку їх функціонування, таку як географічна розподіленість та передача даних через мережі, критичність надійного функціонування бізнес-процесів, забезпечення конфіденційності, повноти, точності та дійсності інформації, обмеження доступу до даних і систем, наявність та функціонування внутрішніх механізмів контролю, їх моніторинг та аудит.

Використання поетапного отримання та аналізу експертної інформації дозволяє визначити перелік критеріїв, які входитимуть в модель гармонізованого стандарту. Для представлення моделі залишилось визначити порядок їх слідування в стандарті. Зважаючи на аналіз структури стандартів CobIT і ISO/IEC, доцільним буде використати підхід від загальних питань до більш конкретних, від ідентифікації загроз та ризиків до конкретних вимог щодо забезпечення інформаційної безпеки корпоративних інформаційних систем та мереж. Таким чином отримаємо наступну структуру моделі гармонізованого стандарту:

1. Визначення інформаційної архітектури
2. Оцінка управління IT ризиками
3. Забезпечення IT-ресурсами
4. Забезпечення безперервності обслуговування
5. Загальні питання інформаційної безпеки
6. Відповідальність за інформаційні активи
7. Безпека в процесах розробки і підтримки
8. Планування та прийом систем до експлуатації
9. Управління безпекою мереж
10. Криптографічні засоби управління
11. Прикладні питання інформаційної безпеки
12. Управління доступом користувачів
13. Безпека персоналу: звільнення та переміщення
14. Управління доступом до додатків і інформації
15. Моніторинг та оцінка внутрішніх механізмів контролю

Висновок

Таким чином, гармонізований стандарт відповідає світовим підходам у забезпеченні інформаційної безпеки комп'ютерних систем та мереж, базуючись на міжнародних стандартах та вимогах (CobIT, ISO/IEC, COSO), має комплексну структуру, розглядає як загальні питання, такі як ідентифікація загроз та ризиків, так і конкретні вимоги щодо забезпечення інформаційної безпеки корпоративних інформаційних систем (ERP) та мереж, а також, завдяки проведенню розгорнутого попереднього аналізу вимог та можливості конкретної реалізації в найбільш поширених промислових ERP-системах, має чітку спрямованість на забезпечення інформаційної безпеки в системах управління ресурсами підприємств.

Література

1. Анохин А.М., Глотов В.А., Павельев В.В., Черкашин А.М. Методы определения коэффициентов важности критериев – "Автоматика и телемеханика", 8, 1997, с 3–35.
2. Гуткин Л.С. Оптимизация радиоэлектронных устройств по совокупности показателей качества. Москва: Радио, – 1975 – 367 с.

Получено 03.04.2008

 ISSN 1562-9945