які підключаються до ProM.

Істотним мінусом ProM є обмежена документація щодо використання вбудованих модулів, які підключаються. Також варто сказати про відсутність повноцінного інтерфейсу командного рядка, що робить застосування ProM в автоматизованому режимі мало можливим, проте даний недолік не є суттєвим.

ОРГАНІЗАЦІЯ ЕЛЕКТРОННОЇ ЗВІТНОСТІ ЧЕРЕЗ ІНТЕРНЕТ

О.О. Денісова, *к.е.н., доцент*

ДВНЗ «Київський національний економічний університет ім. В. Гетьмана»

Розглядаються задачі і проблеми формування і пересилки через Інтернет електронної звітності. Визначено способи захисту інформації, що передається через Інтернет, і забезпечення довіри між учасниками комунікацій

Звітність – єдина система даних про майновий і фінансовий стан компанії та про результати її господарської діяльності протягом звітного періоду, що складається на основі даних бухгалтерського обліку за встановленими формами. Як правило, звітність подається фізичним або юридичним особам, зовнішнім стосовно компанії. Це можуть бути власники (акціонери) компанії, державні органи (зокрема, для оподаткування і статистичного обліку), кредитні та інвестиційні організації, постачальники товарів і послуг, клієнти компанії, її співробітники. При цьому переслідуються цілі підвищення ефективності управління компанією та її відкритості і прозорості для клієнтів, акціонерів і партнерів.

Нині існує три варіанти передачі звітності – в паперовому вигляді, електронна звітність на машинних носіях з дублюванням на папері і звітність через Інтернет. Останній варіант є найшвидшим і найзручнішим.

У процесі організації електронної звітності через Інтернет можна виокремити два взаємопов’язані етапи – формування звітності та її публікація (пересилка).

Головними задачами формування електронної звітності є такі:

– ініціація звітності – створення звітів за певним розкладом або генерування звітів у відповідь на певні заздалегідь визначені бізнес-події. Автоматичне планування звітів часто зустрічається в бухгалтерських програмних пакетах. Запуск звітності бізнес-подіями реалізувати складніше, оскільки це потребує перебудови бізнес-процесів згідно з ролями, правилами і маршрутами. Автоматичне генерування і поширення звітів вимагає зберігання параметрів запитів щодо звітів для повторного їх використання, підтримки списків адресатів, кодифікації бізнес-подій і подій фіскального календаря, що запускають формування звітів;

– керування бібліотеками звітів: звіти зберігаються у вигляді файлів популярних форматів (HTML/XML, електронних таблиць або ін.). Сервери, що зберігають ці файли, виконують роль бібліотек – допомагають користувачеві у пошуку необхідних йому звітів. До їх функцій також входить систематизація звітів, керування версіями, опрацювання звітів (англ. *report mining*) і пошук інформації у звітах;

– перегляд і випуск звітів: список адрес і профілі безпеки визначають осіб, які мають доступ до звітів, і припустимі операції (перегляд, друк, знищення, збереження в інших форматах).

Технологічна інфраструктура електронної звітності вимагає наявності одного або більше спеціалізованих серверів для керування запитами щодо звітів, вибраних з урахуванням максимального навантаження у «пікові» періоди, засобів маршрутизації запитів до вітрини (сховища) даних або до оперативної бази даних залежно від специфіки запиту.

Предметом домовленості між учасниками комунікацій має бути формат файлів, що формуються для передачі. Державні органи регламентують формат документів, які вони приймають в електронному вигляді. В інших випадках вибирають поширені формати (.doc, .pdf). Однак, така практика ускладнює аналіз одержаних даних. Гарною альтернативою може стати використання як єдиного формату публікацій розширюваної мови бізнес-звітності XBRL, що ґрунтується на XML.

Відповідний стандарт пропонує вирішення проблеми ідентифікації даних за допомогою таксономій – словників, що містять визначення термінів бізнес-звітів, зрозумілі комп'ютеру, а також відношення між ними і зв'язки, що пов'язують їх з людиночитабельними ресурсами (метаданими). Таким чином визначаються елементи, що можуть використовуватись в реальних документах. Пакет специфікацій XBRL призначений для швидкого пошуку звітної інформації і наступного добування значень окремих показників. Це надає можливість не лише публікувати і передавати, а й автоматизовано порівнювати та аналізувати фінансову і ділову звітність окремих компаній. При цьому слід зазначити, що XBRL не встановлює стандарти на обсяг даних і вміст звітів, що розташовуються в Інтернеті, це прерогатива самих компаній, які створюють певний звіт.

Вибір способу передачі підготовленої електронної звітності адресату залежить від її регулярності і призначення. В разі подачі регламентованої звітності державним органам файли можуть передаватись або безпосередньо на адресу одержувача, або оператору зв'язку. У відповідь компанія одержує підтвердження про доставку, що має юридичну силу, а час одержання звіту є часом його здачі.

Оператор зв'язку відіграє роль посередника, він забезпечує коректний документообіг між компанією і державними органами як електронний нотаріус. Іншими словами, в разі виникнення спірних питань оператор зв'язку може підтвердити факт доставки і відправки документів.

Нині пропонується два способи взаємодії подавця звітності з посередником: передача зашифрованих даних відкритим каналом зв'язку або незашифрованих даних закритим каналом зв'язку. Перший спосіб має безумовні переваги, оскільки є найбільш захищеним. Якщо посередник є довіреною особою, може виконуватись депонування ключа – передача йому приватного ключа для моніторингу зашифрованих комунікацій та можливого відновлення ключа.

Якщо оператор зв'язку у схемі взаємодії відсутній, факт доставки звітності може додатково перевірятись за допомогою «квитовки» – порівняння опису відправленого документа з підтвердженням про його одержання, що надходить у відповідь.

Документи електронної звітності, що передаються через Інтернет, повинні захищатись криптографічними методами і мати цифровий підпис. Систему захисту інформації легше організувати при наявності єдиного центрального органу, до якого передаються електронні документи. Державні органи в разі готовності приймати електронну звітність беруть на себе функції адміністрування ключів. Якщо ж звітність передається у відповідь на запит зацікавленої особи, необхідне залучення адміністрації сертифікації – довіреної третьої особи, яка накладає свій цифровий підпис на публічний ключ учасника системи звітності і пересвідчує, що даний публічний ключ належить легітимному власнику і не скомпрометований. Таким чином вирішується проблема автентифікації особи, що надала для застосування свій публічний ключ електронною поштою або через сервер ключів.

У загальному випадку користувачі можуть дотримуватись однієї з моделей довіри: пряма довіра, ієрархічна довіра та «павутина довіри», що охоплює дві попередні моделі. Сертифікат може завірятись або безпосередньо, або через певну ієрархічну низку завірителів аж до безпосередньо довіреного сертифікатора (мета-сертифікатора), або певною групою сертифікаторів. Додаткове обґрунтування дають ідеї, що довіра є прерогативою очевидця і чим більше інформації, тим краще.

Захист електронних документів, що передаються, та забезпечення довіри між учасниками комунікацій тісно пов'язані з проблемою керування ключами усередині компанії. Для засвідчення автентичності документів може застосовуватись так званий корпоративний ключ – приватний ключ, призначений для підписування інших ключів, або поділ одного ключа на частини, окремі для кожного користувача з певної групи, таким чином, щоб скористатися ним можна було тільки за умови складання певної кількості частин разом.

З урахуванням вищесказаного, можна зробити висновок, що для організації звітності через Інтернет потрібно здійснити проекти з перебудови бізнес-процесів компаній і створення інфраструктури обміну і захисту даних.