УДК 004.422

О.Г. МАНОХІН
Л.В. МАНОХІНА
Г.Ф. СОЛОВКО
О.В. МАКСЮТА
ДГЦУ

"Експерт – ДГЦУ – Митниця". Етап II

"Електронна митниця" – це система, яка дозволяє кожному суб'єкту і кожному підприємцеві працювати без використання паперів, а також дає можливість мінімізувати людський фактор, можливі корупційні прояви. "Адже людина може, не виходячи зі свого офісу, завдяки системі "Електронна митниця" здійснити митне оформлення дорогого вантажу". (І. КАЛЄТНІК)

У 2011 році Державна митна служба України на виконання Указу Президента про реформування митної служби почала реалізацію пілотного проекту з декларування, митного контролю та оформлення товарів із застосуванням електронних декларацій. Цей проект здійснюється на базі Київської регіональної, Київської обласної та Південної митниць. У ньому беруть участь п'ять компаній, включених до реєстру підприємств, до товарів яких можна застосовувати процедуру електронного декларування. Голова Державної митної служби України Ігор Калєтнік прогнозує, що до кінця цього року "Електронна митниця" запрацює на повну силу. Митниці, задіяні в проекті, будуть фіксувати у відповідних протоколах проблемні питання, які можуть виникнути під час його реалізації.

У ДГЦУ здійснюється розробка системи електронного декларування за групами товарів та видами робіт, що належать до сфери експертної діяльності нашої організації. Протягом року буде здійснено поетапне переведення всіх дозвільних документів, які видає ДГЦУ, в електронний вигляд, а повністю запустити систему електронного декларування планується до кінця 2011 року.

У 2010 році в дослідну експлуатацію запущено першу чергу системи – автоматизоване робоче місце (АРМ) експерта-гемолога з декларування товарів з декоративного каменю.

У частині створення інформаційного забезпечення АРМ проводяться:
- розробка багаторівневих підпорядкованих словників з можливістю введення кінцевих даних на робочих місцях (довідники кар'єрів, адресні довідники (експертів, замовників);
- розробка базових фільтрів для аналізу даних;
- розробка базових вихідних форм звітності;
- розробка словників для роботи БД (типів продукції, найменувань каменів, одиниць вимірів).

У частині бухгалтерського обліку відпрацьовано й реалізовано механізм проведення оплат за експертизу. У структурі БД для кожного клієнта ведеться своя історія фінансової

діяльності: всі надходження коштів (вносяться зі знаком "+") та оплати (зі знаком "-") фіксують з кодом оператора (експерт, керівник, бухгалтер) у момент закриття документа. Таким чином, ми сподіваємося повністю вирішити питання кредиторської заборгованості по ДГЦУ.

У частині розвитку системи розроблено структури баз даних за АРМ-ами другої черги – для решти напрямів експертної діяльності організації.

Для здійснення обміну інформацією між Державною митною службою України та ДГЦУ найближчим часом буде узгоджено і підписано протокол погодження щодо реквізитів та способу обміну інформацією.

Спершу обмін інформацією між ДГЦУ і митницею передбачається проводити у форматі XML у відкритому вигляді за допомогою електронної пошти. Формат XML – потужний засіб, який часто застосовують для обміну даними через Інтернет. Але, на жаль, сам по собі він не забезпечує необхідний захист даних, які "перевозить". Іншими словами, існують серйозні проблеми безпеки при застосуванні формату XML (утім, як і при використанні інших форматів).

Формат XML може бути легко використаний для передачі повідомлень-транзакцій між клієнтом і СУБД, конфіденційних чи напівконфіденційних відомостей про фізичних осіб, відомостей про електронні декларації або просто для передачі закритих документів. Однак при цьому потрібно забезпечити захист інформації від ненавмисних чи навмисних помилок як з боку користувачів інформаційних систем, так і під час передачі каналами зв'язку. Захист повинен ґрунтуватися на виконанні таких функцій:

– аутентифікації взаємодіючих сторін;
– підтвердженні достовірності та цілісності інформації;
– криптографічному закритті даних, що передаються.

Для забезпечення такого захисту інформації доцільно застосовувати методи електронного цифрового підпису (ЕЦП) та шифрування даних. Причому, як правило, ЕЦП забезпечує аутентифікацію, підтвердження достовірності та цілісності, а закриття даних досягається шифруванням.

Режим і порядок обміну запроваджується митницею та визначається її можливостями, нині обмін здійснюється раз на добу. Згодом можливе прискорене проходження документів. Система, яку розробляє ДГЦУ, потенційно може передавати дозвільні документи на митницю в он-лайновому режимі.

Передача інформації експертами, системою, митницею здійснюється відкритими каналами Інтернету, тому питання захисту інформаційних ресурсів набуває все більшого значення. Щоб забезпечити повноцінний захист інформації, необхідно провести повний спектр робіт в галузі захисту інформації. До нього входять як програмно-апаратні комплекси захисту інформації, так і використання спеціальних підходів з питань доступу до системи і до захисту інформації.

Щоб захистити комп'ютерні мережі або окремі машини від несанкціонованого доступу, в системі використовують ефективний міжмережевий екран, або firewall, який дозволяє ідентифікувати абонента (статичну адресу, пароль), контролювати обсяг отриманої інформації та запобігати несанкціонованому проникненню. Клієнтська частина системи побудована як Desktop-додаток, а тому не використовує протокол HTTP. Це, в свою чергу, в декілька разів підвищує безпеку програми за рахунок усунення можливості використання зловмисниками численних слабких місць стандартних інтернет-протоколів.

Для проведення сервісних робіт (наприклад, при віддаленому адмініструванні системи) застосовують VPN (Virtual Private Network – логічна мережа, що створюється поверх іншої мережі, наприклад, Інтернет) з використанням іншого протоколу типу PPTP і протоколу перевірки пароля CHAP. Включено режим шифрування даних.

PPTP – тунельний протокол типу "точка-точка", що дозволяє комп'ютеру встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній незахищеній мережі. PPTP вміщує (інкапсулює) кадри PPP в IP-пакети для передачі глобальною IP-мережею, наприклад, Інтернет.

CHAP – широко поширений алгоритм перевірки автентичності, що передбачає передачу не самого пароля користувача, а непрямих відомостей про нього. При використанні CHAP сервер віддаленого доступу відправляє клієнту рядок запиту. На основі цього рядка і пароля користувача клієнт обчислює хеш-код MD5 (*англ.* – Message Digest-5) і передає його серверу. Хеш-функція є алгоритмом одностороннього (незворотного) шифрування (перетворення), оскільки значення хеш-функції для блоку даних легко обчислити, а визначити вихідний блок за хеш-кодом з математичної точки зору неможливо за прийнятний час. Сервер, для якого є доступним пароль користувача, виконує ті самі розрахунки і порівнює результат з хеш-кодом, отриманим від клієнта. У разі збігу облікові дані клієнта віддаленого доступу вважаються справжніми.

Конфігурацію та характеристики віртуальної приватної мережі багато в чому визначає тип застосовуваних VPN-пристроїв. За способом технічної реалізації в системі є можливість використовувати VPN-з'єднання на основі:

- маршрутизаторів;
- міжмережевих екранів;
- програмних рішень;
- спеціалізованих апаратних засобів із вбудованими шифропроцесорами.

VPN на основі маршрутизаторів. Цей спосіб побудови VPN передбачає застосування з локальної мережі, проходить через маршрутизатор, отже, цілком природно покласти на нього і завдання шифрування. Приклад обладнання для VPN на маршрутизаторах – пристрої компанії "Cisco Systems".

VPN на основі міжмережевих екранів (МЕ). МЕ більшості виробників підтримують функції тунелювання і шифрування даних, наприклад, продукт "Fire Wall-1" компанії "Check Point Software Technologies". При використанні МЕ на базі ПК потрібно пам'ятати, що таке рішення підходить тільки для невеликих мереж з невеликим обсягом переданої інформації. Недоліками цього методу є висока вартість рішення в перерахунку на

одне робоче місце і залежність продуктивності від апаратного забезпечення, на якому працює МЕ.

VPN на основі програмного забезпечення. VPN-продукти, реалізовані програмним способом, з точки зору продуктивності поступаються спеціалізованим пристроям, проте володіють достатньою потужністю для реалізації VPN-мереж. Слід зазначити, що у випадку віддаленого доступу вимоги до необхідної смуги пропускання невеликі. Тому суто програмні продукти легко забезпечують продуктивність, достатню для віддаленого доступу. Без сумніву, позитивною рисою програмних продуктів є гнучкість і зручність у застосуванні, а також відносно невисока вартість.

VPN на основі спеціалізованих апаратних засобів. Головна перевага таких VPN – висока продуктивність, оскільки швидкодія зумовлена тим, що шифрування в них здійснюється спеціалізованими мікросхемами. Спеціалізовані VPN-пристрої забезпечують високий рівень безпеки, однак вони дорогі.

Який із цих варіантів з'єднань буде вибрано для роботи в системі, виявиться в процесі взаємодії з митницею.

Активно триває розробка і запуск у дослідну експлуатацію АРМ-ів другої черги системи електронного декларування:

– АРМ експерта-гемолога алмазного відділу;
– АРМ експерта-гемолога дорогоцінного та напівдорогоцінного каміння;
– АРМ експерта-гемолога з технічних алмазів та інструментів;
– АРМ експерта з обслуговування Кімберлійського процесу.

Для кожної системи розробляють свої структури записів БД, а також свої алгоритми збору і обробки інформації. Спільними для всіх є бази даних клієнтів – замовників експертизи, словники (мір і ваги, назв міст, вулиць тощо)

Процедури створення електронних документів для кожного з АРМ-ів розробляють за аналогією до правил документообігу, прийнятим при оформленні паперових документів для цих видів при проходженні митних процедур.

Як повідомлялося, впровадження електронного декларування дозволить зменшити суб'єктивний фактор, а відповідно і корупційну складову в роботі представників митних органів, максимально спростити процедуру оформлення, скоротити часові і фінансові витрати на ведення зовнішньоекономічної діяльності.