УДК 351.713:004.056.(477)

Т.В. СУБІНА, молодший науковий співробітник Науково-дослідного центру з проблем оподаткування Національного університету ДПС України

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕЛЕКТРОННОЇ ЗВІТНОСТІ В ОРГАНАХ ДЕРЖАВНОЇ ПОДАТКОВОЇ СЛУЖБИ УКРАЇНИ

Анотація. *У статті розглянуто деякі засоби захисту інформаційної безпеки, що застосовуються при електронному оподаткуванні в органах державної податкової служби України.*

Сучасний період розвитку цивілізації на планеті визначається переходом від індустріального до постіндустріального інформаційного суспільства. Цей процес супроводжується впровадженням інформаційно-комунікаційних технологій в усі сфери суспільного життя, зокрема в центральні та місцеві органи виконавчої влади.

Інтеграція України у світовий інформаційний простір є актуальним питанням сьогодення. Наша держава виходить на міжнародну арену, що має демократичне, суверенне, інформаційне суспільство.

У даному напрямі досліджень привертають увагу праці сучасних українських учених В. Брижка, В. Гавловського, Р. Калюжного, В. Цимбалюка, В. Шамрая, М. Швеця, В. Шкарупи та ряду інших. А також праці російських учених Г. Артамонова, І. Бачила, В. Іноземцева, В. Копилова, В. Лопатіна В. Отрековського, А. Ракітова, І. Сиголяна, С. Черемкіна та інших.

З’ясування сутності та змісту категорії “інформаційне суспільство” у вітчизняному правознавстві повинно сприяти формуванню не тільки політичної, економічної та правової культури, а й загальної культури народу України, суспільства, окремих індивідів. Особливу увагу на усвідомлення сутності категорії “інформаційне суспільство” потрібно звернути не тільки науковцям, а й тим, від кого залежить подальший поступ розвитку держави – менеджерам, управлінцям, державних діячам, представникам законодавчої та центральної виконавчої влади, керівникам органів місцевого самоврядування, інтелектуальній еліті, тим, від кого залежить формування та реалізація державної інформаційної політики, поступу країни до передових світових стандартів соціального прогресу, що формується завдяки здобуткам науково-технічного прогресу у сфері інформатики, комп’ютерної техніки, електронних засобів телекомунікації, зв’язку [1, с. 92].

Для того щоб Україна стала повноправним членом Європейського Союзу, СОТ та увійшла у світовий інформаційний простір, потрібно врегулювати ряд проблем, зокрема, забезпечення інформаційної безпеки як на внутрішньому, так і на зовнішньому рівнях, що потребує збільшення державної фінансової, бюджетної підтримки.

Наповнення бюджету країни, а отже, і функціонування усієї держави та суспільства в цілому, значною мірою залежить від ефективності роботи податкової служби. Органи державної податкової служби України (далі – ДПС України) в своїй роботі враховують усі зміни в економіці, на інформаційному та нормативно-правовому полі [2].

ДПС України є нерозривною частиною державного організму, що враховує рівень її впливу на економічні процеси в країні, розвиток заявленої державою соціально орієнтованої ринкової економіки [3, с. 16]

У зв’язку з розвитком інформаційно-комунікаційних технологій платники податків

© Т.В. Субіна, 2009

мають можливість подавати податкову звітність в електронному вигляді до органів ДПС України відповідно до наказу Державної податкової адміністрації України (далі – ДПА України) “Про затвердження формату (стандарту) електронного документа звітності платників податків” [4].

Податкова звітність є одним із видів державної. Вона складається з: декларації з податку на прибуток підприємства; податкової декларації з податку на додану вартість; розрахунку акцизного збору; звітів щодо обігу спирту, алкогольних напоїв та тютюнових виробів та інструкцій щодо їх заповнення, звіту про суму нарахованого збору на розвиток виноградарства, садівництва і хмелярства; податкової звітності результатів спільної діяльності на території України без створення юридичної особи. Таким чином, податкова звітність дозволяє обчислити сплачені податки та інші обов’язкові платежі, а також прогнозувати і моделювати податкові надходження.

Органами ДПС України реєстри податкової звітності ведуться у документальному або електронному вигляді за вибором платника податку. Ці документи повинні зберігатися платником податку протягом строку давності. Платник податку має право за власним бажанням подавати до органів ДПС України реєстри отриманих і виданих податкових накладних. Реєстри можуть подаватися відповідно до Наказу ДПА України № 30 від 26.01.2007 р. в електронному вигляді на магнітних носіях (магнітних дисках, флеш-картах, компакт-дисках тощо) у форматі, затвердженому ДПА України, за допомогою телекомунікаційних мереж загального користування (on-line, off-line, Utel або інший провайдер зв’язку, який гарантує доставку пакета звітних документів платника до органів ДПС протягом однієї години) з використанням надійних засобів електронного цифрового підпису (далі – ЕЦП) за умови отримання їх у порядку та із забезпеченням захисту інформації з копіями документів на паперових носіях поштовими відправленнями тощо [5].

Податкова звітність приймається безпосередньо від платника через відділ обробки та ведення податкових документів без попередньої перевірки зазначених у ній показників. Відмова працівника прийняти податкову декларацію з будь-яких причин або висунення ним будь-яких умов щодо такого прийняття (включаючи зміну показників такого звіту, зменшення або скасування від’ємного значення об’єктів оподаткування, сум бюджетних відшкодувань, незаконного збільшення податкових зобов’язань, візування звітності галузевим підрозділом тощо) забороняється та розцінюється як перевищення службових повноважень таким працівником, що тягне за собою дисциплінарну та матеріальну відповідальність [6].

Значними перевагами електронної звітності є наступне: економія робочого часу платників податків, а також їхніх коштів на придбання бланків звітних документів (не потрібно відвідувати податкову інспекцію, купувати бланки звітності); гарантія автоматичної перевірки підготовлених документів на наявність арифметичних помилок та описок; можливість оперативного оновлення форматів подання документів в електронному вигляді телекомунікаційними каналами зв’язку (у разі зміни форм податкових декларацій, інших документів, які є підставою для нарахування і сплати податків, або при введені нових форм декларацій платник податків автоматично отримує можливість оновити версії форматів), можливість отримати інформацію щодо стану розрахунків стосовно сплати податків і заборгованості перед бюджетом. Сьогодні цілий ряд країн, таких як: США, Канада, Швеція, Бельгія, Люксембург, Росія, перейшли на безпаперову технологію подання бухгалтерської та податкової звітності через Інтернет [7, с. 2].

Звітність в електронному вигляді є вигідною як для органів ДПС України, так і для платників. З одного боку, органи ДПС України отримують звітні документи від платників податків, практично не витрачаючи часу на їх занесення до електронної бази даних. З іншого, і платники податків зацікавлені в процесі подачі звітності в електронному вигляді. Звітність до податкових органів може бути передана безпосередньо з робочого місця, що знаходиться в офісі платника, без черг, без труднощів, пов’язаних з передачею звітності у дні її масового подання. Податкова звітність автоматично перевіряється на наявність у звітних документах помилок, що дає платнику можливість виявляти і виправляти помилки самостійно, до подачі звітних документів до податкових інспекцій. Для таких перевірок у системах підготовки звітності закладені спеціальні алгоритми. Відпадає також потреба і в самих бланках звітності.

Під час передачі податкової електронної інформації використовуються системи криптографічного захисту інформації, які розроблялися провідними науковими установами України. Серед таких систем захисту потрібно відзначити:

- криптографічну систему захисту інформації, що має гриф обмеження “Для службового користування”. Система отримала позитивний експертний висновок фахівців ДСТСЗІ СБУ, пройшла дослідну експлуатацію в ДПА України у м. Києві, поширена на декілька областей України;
- систему сеансового захисту роботи авторизованого користувача з базами даних, що працює за технологією Java в системі on-line;
- систему збору податкової звітності “Бест-Звіт”, яка працює в системі Offline, яку плануються безкоштовно встановлювати на робочому місці бухгалтера підприємства-платника податків [8, с. 494-495].

При передаванні податкових документів до органів ДПС України здійснюється їх шифрування. Відповідно до нормативного документа технічного захисту інформації 2.5-004 – 99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 28.04.1999 р. № 22, використання симетричних криптоалгоритмів (шифрування повідомлень) і несиметричних криптоалгоритмів (накладання електронного цифрового підпису) відповідно до вимог Закону України від 22.05.2003 р. № 852-IV “Про електронний цифровий підпис” є необхідною та достатньою вимогою забезпечення конфіденційності, цілісності інформації, що використовується для обліку [9, с.17].

Зокрема, у Положенні про здійснення криптографічного захисту інформації в Україні зазначено, що криптографічний захист – це вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Засобом криптографічного захисту інформації є програмний, апаратно-програмний, апаратний або інший засіб, призначений для криптографічного захисту інформації.

Порядок розроблення, виготовлення, розповсюдження, експлуатації, збереження, використання, випробування, сертифікації та допуску до експлуатації криптосистем (сукупність засобів криптографічного захисту інформації), необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та передається [10, с. 4].

Для забезпечення єдиної технології приймання та обробки електронної податкової звітності повинні виконуватися субпроцеси: наприклад, формування та ведення бази даних сертифікатів відкритих ключових даних платників податків, що подають податкову звітність в електронному вигляді [11].

Подаючи податкову звітність в електронному вигляді до органів ДПС України, платникам податків необхідно звернутися до державної податкової інспекції за місцем реєстрації, для фізичних осіб – за місцем проживання. Платник податків отримує в ДПІ за місцем реєстрації або на веб-сайті ДПА України //www.sta.gov.ua чи ДПА у м. Києва //www.kyivsta.ua текст Договору, а також в акредитованому центрі сертифікації ключів, з якими ДПА України укладено договір, для подання податкової звітності платниками податків із застосуванням ЕЦП, – посилені сертифікати відкритих ключів посадових осіб підприємства, що мають право підпису (керівника, бухгалтера), печатки підприємства та безкоштовне програмне забезпечення шифрування та накладання ЕЦП, яке має сертифікат відповідності. Платник податків фізична особа – суб’єкт підприємницької діяльності може обмежитися одним ЕЦП.

Розглянемо перелік акредитованих центрів сертифікації ключів за станом на квітень 2008 року, з якими ДПА України укладено договір для надання податкової звітності платниками податків із застосуванням ЄЦП.

Такими організаціями є ЗАТ “ІВК”, код ЄДРПОУ 33406085, “Український сертифікаційний центр”, код ЄДРПОУ 33406510, ТОВ “Арт-Мастер” код ЄДРПОУ 30404750, а також ТОВ “Українські спеціальні системи”, код ЄДРПОУ 32348248. Прикладом тарифів за послуги акредитованого центру сертифікації ключів є ТОВ “Арт-Мастер” Генерація особистого ключа із записом особистого ключа на компакт-диск (CD-R), формування посиленого ключа Сертифіката відкритого ключа в офісі виконавця, обслуговування посиленого сертифіката відкритого ключа протягом 12 місяців (анулювання, блокування). Відповідно разом пакет “Звітність”, акція “Спокій бухгалтера” – 5,00 грн., вартість з ПДВ, акція 3 за ціною 1-го – 49,00 грн. з ПДВ, “Обмежаний” 486,00 грн. з ПДВ, “Необмежаний” – 594,00 грн. із ПДВ. А також існують додаткові послуги, зокрема: відновлення посиленого Сертифіката відкритого ключа, зміна реквізитів у посиленому сертифікаті відкритого ключа, зміна парольної фази (при голосовій автентифікації), видача дубліката та інші.

Автентифікація – процедура встановлення належності користувачеві інформації в системі пред’явленого ним ідентифікатора.

Ідентифікація – процедура розпізнавання користувача в системі, як правило, за допомогою вже визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом [12].

Автентифікацію можна поділити на такі типи: автентифікація абонента, автентифікація абонента, що належать до цієї групи, автентифікація документів, що зберігаються в машинних носіях.

Автентифікація документів – це безпаперова документація, що дає ряд переваг при обміні документа (наказ, розпорядження, лист, постанова тощо) мережею зв’язку або на машинних носіях. Проблема автентифікації є актуальною в обчислювальних мережах, електронних системах управління, електронній комерції і взагалі там, де треба переконатись у справжності отриманого каналами зв’язку або на машинних носіях.

Метою автентифікації є захист від можливих видів зловмисних дій, серед них:

• активне перехоплення зловмисників, що підключилися до мережі, перехоплює документи (файли);

• маскування абонента-зловмисника (виступає від імені абонента передавача);

• ренегатство – абонент-передавач заявляє, що не надсилав повідомлення абоненту одержувачу, хоча насправді надсилав;

• переробка – абонент-одержувач змінює документ і стверджує, що цей змінений документ отриманий від абонента-передавача;

• підміна – абонент-одержувач формує новий документ і заявляє, що отримав його від абонента-передавача;

• повтор – абонент-зловмисник повторює раніше переданий документ, який абонент-передавач надіслав абоненту одержувачу.

Цими діями зловмисники завдають значної шкоди функціонуванню банків, комерційних структур, державних підприємств, приватним особам, що застосовують у своїй діяльності комп’ютерні інформаційні технології. Крім того, можливість зловмисних дій підриває довіру до комп’ютерної технології щодо аутентифікації повідомлень у мережі, тому потрібно передбачити надійний захист від усіх злочинних дій [13].

Акредитований центр сертифікації ключів ЗАТ інфраструктури відкритих ключів забезпечує надання послуг ЕЦП. Даний Центр сертифікації ключів надає посилені сертифікати відкритих ключів, що дозволяє використовувати технологію ЕЦП в системі державного управління, а також комерційному та в державному секторах економіки України. У складі Акредитованого Центру сертифікації ключів використовуються унікальні програмно-апаратні рішення, які забезпечують високий рівень надійності захисту інформації.

Надання послуг ЕЦП передбачає: використання засобів ЕЦП; обслуговування сертифікатів (формування, блокування, поновлення, скасування); надання допомоги при генерації ключів абонентів; надання відомостей щодо статусу сертифіката абонента; надання позики часу; можливість криптографічного захисту інформації, переданої у відкриті мережі, завдяки направленому шифруванню; забезпечення цілодобового супроводу абонентів; консультування заявників.

Управління центрів надає послуги щодо захисту електронної пошти щодо документів ДПА України, ДПІ [//www.asta.gov.ua]. Центр сертифікації ключів зобов’язаний:

• забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;

• забезпечувати захист персональних даних, отриманих від підписувача, згідно із законодавством;

• встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;

• своєчасно скасовувати, блокувати та поновлювати сертифікати ключів та інше.

Сертифікат ключа містить такі обов’язкові дані: найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру); зазначення, що сертифікат виданий в Україні; унікальний реєстраційний номер сертифіката ключа; основні дані (реквізити) підписувача – власника особистого ключа; дату і час початку та закінчення строку чинності сертифіката; відкритий ключ; найменування криптографічного алгоритму, що використовується власником особистого ключа; інформацію про обмеження використання підпису.

Посилений сертифікат ключа, крім обов’язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника.

Суб’єктами правових відносин у сфері послуг ЕЦП є: підписувач; користувач; центр сертифікації ключів; акредитований центр сертифікації ключів; центральний засвідчувальний орган; засвідчувальний центр органу виконавчої влади або іншого державного органу; контролюючий орган.

ЕЦП за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- ЕЦП підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

ЕЦП не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа [14].

Закон України “Про електронний цифровий підпис” поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

Технологія ЕЦП така: інформація, яку потрібно підписати, обробляється спеціальною програмою із використанням так званого закритого ключа і надсилається електронною поштою. Одержувач інформації має власний ключ, за допомогою якого можна переконатися, що інформація надійшла без пошкоджень, що відправник підписав саме це повідомлення і що там стоїть саме його підпис. Важливо, що при “виготовленні” та перевірці підпису використовуються спеціальні криптографічні перетворення, а от оцифроване зображення підпису на папері електронним цифровим підписом не вважається. Після роздрукування він втрачає свою силу [15].

На нашу думку, послуги криптографічного захисту повинні надаватися безкоштовно, оскільки це одна із складових забезпечення інформаційної безпеки. У Конституції України є ряд статей (зокрема, ст. ст. 17, 32, 34), що визначають забезпечення інформаційної безпеки як одну з найбільш важливих функцій держави і повинні стати основою розвитку інформаційного суспільства.

Із зазначеного вище можна зробити висновок, що впровадження в органи ДПС України інформаційно-комунікаційних технологій дозволяє систематизувати інформаційний реєстр платників податків, покращити співпрацю з платниками податків, прискорити обробку податкових даних; скоротити кількість перевірок і підвищити їх якість внаслідок оперативного відбору підприємств для перевірок тощо.

Забезпечення інформаційної безпеки щодо здійснення електронної звітності має багато не вирішених питань. Так, платники податків не повинні обмежуватися одним сертифікованим відкритим ключем ЕЦП. Наприклад, якщо податкову звітність у паперовому варіанті потрібно підписати кільком особам (керівнику, бухгалтеру та іншим), накладати 2 та більше електронних цифрових підписів на один електронний документ.

Таким чином, одним з основних завдань держави є вирішення питання щодо ЕЦП та формування умов щодо використання сертифікованих інформаційних, технологічних і технічних засобів захисту електронної звітності та забезпечення інформаційної безпеки в органах ДПС України і держави в цілому

Використана література

1. Швець М., Калюжний Р., Гавловський В., Брижко В. Україна на шляху до Інформаційного суспільства // Правова інформатика. – № 1/2003. – С. 92-100.

2. Розвиток інформаційної інфраструктури як складової програми модернізації державної податкової служби України. – Режим доступу: //www.sta.gov.ua/news.php3?1472

3. Ф.О. Ярошенко Трансформація державної податкової служби України : монографія / Ф.О. Ярошенко. – Ірпінь: Національна академія ДПС України, 2004. – С. 16.

4. Про затвердження формату (стандарту) електронного документа звітності платників податків : Наказ ДПА України від 03.05.2006 р. № 242.

5. Порядок ведення реєстру отриманих та виданих податкових накладних : Наказ ДПА України : зареєстровано в Міністерстві юстиції України 18 липня 2005 р. за № 770/11050.

6. Про затвердження нової редакції Порядку приймання та комп’ютерної обробки звітних документів платників податків у ДПІ районного рівня та СДПІ по роботі з ВПП : Наказ ДПА України від 02.12.2004 р. № 691.

7. Актуальні матеріали з питань застосування податкового законодавства з податку на додану вартість. – (ДП “Інформаційно-видавничий центр ДПА України”). – К., 2008. – С. 2.

8. Давидюк В.С Напрями захисту інформації, притаманні специфіці податкової служби : тези доповідей ІІІ Міжнародної науково-практичної конференції “Проблеми впровадження інформаційних технологій в економіці та бізнесі”. – Ірпінь, 2002. – С. 494-495.

9. Подання податкової звітності та реєстрів податкових накладних в електронному вигляді // Вісник податкової служби України. – 2006. – № 47-48(427). – Ст. 80. – С. 17.

10. Положення про порядок здійснення криптографічного захисту інформації в Україні // Офіційний вісник України. – 1998. – № 21. – С. 4.

11. Про затвердження Тимчасового порядку надходження та комп’ютерної обробки податкової звітності платників податків в електронному вигляді до органів ДПС України : витяг з наказу від 26 листопада 2004 року № 672 // Податковий, банківський, митний консультант. – 2004. – № 50.

12. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.2006 р. № 373 // Офіційний вісник України. – 2006. – № 13. – С. 164. – Ст. 878.

13. Задірака В.К. Метод захисту фінансової інформації : навчальний посібник / В.К.Задірака, О.С. Олексик. – Тернопіль : “Збруч”. – 2000. – 460 с.

14. Про електронно-цифровий підпис : Закон України // Відомості Верховної Ради України (ВВР). – 2003. – № 36. – Ст. 276.

15. Що таке електронний цифровий підпис. – Режим доступу : www.tax.vsem.com.ua/index.php?page=news.html&idnn=519

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~