УДК 004.01(0.02)

А. П. Шаўлюкоў (BUiFM@yandex.ru),
доктар эканамічных навук, прафесар
Беларускага гандлёва-эканамічнага
ўніверсітэта спажывецкай кааперацыі

ЭЛЕКТРОННЫЯ ДАКУМЕНТЫ: ПАРАДАК СТВАРЭННЯ І ВЫКАРЫСТАННЯ Ў АРГАНІЗАЦЫЯХ РЭСПУБЛІКІ БЕЛАРУСЬ

У артыкуле раскрыта сутнасць электроннага дакумента і электроннага лічбавага подпісу, працэдура яго атрымання і парадак выкарыстання. У паслядоўным парадку раскрываюцца такія аспекты сертыфікацыі электроннага дакумента, як выпрацоўка ключавой пары, падпісанне электроннага дакумента і праверка электроннага лічбавага подпісу. Аўтар раскрывае сутнасць і значэнне асабістага ключа і адкрытага ключа праверкі электроннага лічбавага подпісу. У артыкуле паказана роля сертыфікаванага сродку электроннага лічбавага подпісу для кантролю над цэласнасцю і аўтэнтычнасцю электроннага дакумента.

The essence of electronic document and the electronic digital signature, the procedure of its receipt and the order of use are set forth in the article. In the consecutive order such aspects of electronic document certification as making of the key pair, the subscription of electronic document and the verification of electronic document are being disclosed. The author opens the essence and importance of the personal key and the public key of electronic digital signature verification. In the article the role of certificate means of electronic digital signature for the control over entireness and authentic of electronic document is shown.

Ключавыя словы: электронны дакумент; агульная частка; асаблівая частка; электронны лічбавы подпіс; штамп часу; ключавая пара; асабісты ключ; адкрыты ключ; падпісанне электронных дакументаў; мабільны электронны лічбавы подпіс; сертыфікат адкрытага ключа; атрыбутны сертыфікат; праверка электроннага лічбавага подпісу.

Key words: electronic document; general part; peculiar part; electronic digital signature; stamp of time; key pair; personal key; public key; signing of electronic documents; mobile electronic digital signature; public key certificate; attribute certificate; verification of electronic digital signature.

Уводзіны

У сучасных умовах усё большае распаўсюджванне атрымліваюць электронныя дакументы. Аднак вельмі часта супрацоўнікі эканамічных службаў арганізацый на маюць базавых ведаў, якія дазваляюць без рызыкі нанясення суб'екту гаспадарання страт выкарыстоўваць электронныя дакументы ў практычнай дзейнасці. Асабліва гэта датычыцца супрацоўнікаў, якія закончылі навучальныя ўстановы нават 10 гадоў таму назад, не гаворачы ўжо пра больш позні перыяд. Гэта абумоўлівае неабходнасць павышэння прафесійных кампетэнцый такіх супрацоўнікаў бухгалтэрый, фінансавых і эканамічных аддзелаў, таксама іншых падраздзяленняў арганізацый. На ліквідаванне такога недахопу ў прафесійнай кампетэнтнасці службовых асобаў арганізацый і накіраваны прапанаваны артыкул.

Электронныя дакументы і электронны лічбавы подпіс. Электронны дакумент – гэта дакумент у электронным выглядзе з вызначанымі заканадаўствам рэквізітамі, якія дазваляюць устанавіць яго цэласнасць і аўтэнтычнасць, што пацвярждаецца сертыфікаванымі сродкамі электроннага лічбавага подпісу. Ён складаецца з дзвюх неад'емных частак: агульнай і асаблівай. Агульная частка электроннага дакумента – гэта непасрэдна сам дакумент з усімі яго рэквізітамі, за выключэннем даты дакумента, рэгістрацыйнага індэкса, рэзалюцыі, адзнакі аб паступленні і іншых рэквізітаў, якія фарміруюцца пасля падпісання дакумента электронным лічбавым подпісам.

Асаблівая частка электроннага дакумента – гэта электронны лічбавы подпіс асоб, якія ажыццявілі ўзгадненне, падпісанне і зацвярджэнне электроннага дакумента, а таксама рэквізіты,

якія фарміруюцца пасля падпісання (дата дакумента, рэгістрацыйны індэкс і інш.). Электронны лічбавы подпіс – гэта паслядоўнасць сімвалаў, якая выпрацоўваецца для дадзенага электроннага дакумента з выкарыстаннем асабістага ключа, правяраецца з выкарыстаннем адкрытага ключа, з'яўляецца рэквізітам электроннага дакумента, служыць для пацвярджэння яго цэласнасці ды праўдзівасці і забяспечвае немагчымасць адмовы ад аўтарства.

Асаблівая частка электроннага дакумента можа ўтрымліваць штамп часу і дадатковыя даныя, патрэбныя для праверкі электроннага лічбавага подпісу і ідэнтыфікацыі электроннага дакумента. Важным элементам асаблівай часткі электроннага дакумента з'яўляецца метка часу, якая ў Законе аб электронным дакуменце і электронным лічбавым подпісе Рэспублікі Беларусь атрымала назву штамп часу. Метка часу – гэта дакументаваная інфармацыя, якая сведчыць пра сувязь кантрольнай характарыстыкі пэўнага інфармацыйнага аб'екта з канкрэтным часам і стварае тым самым доказ існавання гэтага аб'екта ў той момант часу. Зыходзячы з гэтага ў прымяненні да электроннага дакумента штамп часу – гэта рэквізіт электроннага дакумента, які засведчвае дату і час яго стварэння. Дадатковыя даныя ўстанаўліваюцца тэхнічнымі нарматыўнымі актамі.

Як было адзначана вышэй, цэласнасць і аўтэнтычнасць электроннага дакумента пацвярждаецца сертыфікаванымі сродкамі электроннага лічбавага подпісу. Сертыфікаваны сродак электроннага лічбавага подпісу ўяўляе сабой сродак, які мае сертыфікат адпаведнасці патрабаванням тэхнічных нарматыўных прававых актаў у галіне тэхнічнага нармавання і стандартызацыі. Сродак электроннага лічбавага подпісу – гэта праграмны, праграмна-тэхнічны або тэхнічны сродак, з дапамогай якога рэалізуюцца адна або некалькі наступных функцый: 1) выпрацоўка ключавой пары; 2) падпісанне электроннага дакумента; 3) праверка электроннага лічбавага подпісу.

Ключавая пара складаецца з асабістага ключа і адпаведнага яму адкрытага ключа. Асабісты ключ электроннага подпісу, які яшчэ можа называцца закрыты ключ, або ключ электроннага подпісу, – гэта набор сімвалаў, які належыць канкрэтнай асобе і выкарыстоўваецца пры выпрацоўцы электроннага лічбавага подпісу або пры іншым выкарыстанні асіметрычнага алгарытму шыфравання. Адкрыты ключ, які яшчэ называецца публічны ключ, або ключ праверкі электроннага подпісу, – гэта паслядоўнасць сімвалаў, якая адпавядае пэўнаму асабістаму ключу, даступная для ўсіх удзельнікаў сістэмы электроннага дакументаабароту і выкарыстоўваецца для праверкі электроннага лічбавага подпісу.

Асіметрычны алгарытм шыфравання ўяўляе сабой алгарытм крыптаграфічнага ператварэння з дапамогай ключавой пары, у якой адзін ключ дазваляе ажыццяўляць зашыфроўку даных, а другі – расшыфроўку. Крыптаграфічнае пераўтварэнне – гэта ператварэнне інфармацыі, заснаванае на пэўным алгарытме, які залежыць ад падлеглага змяненню параметра (ключа). Крыптаграфічнае пераўтварэнне павінна валодаць ўласцівасцю немагчымасці без ведання дзеючага ключа ўзнаўлення зыходнай інфармацыі па ператворанай, з працаёмкасцю меншай, чым загадзя зададзенай.

Уладальнікам асабістага ключа з'яўляецца арганізацыя або фізічная асоба, якія ажыццявілі выпрацоўку асабістага ключа з выкарыстаннем сертыфікаванага сродку электроннага лічбавага подпісу. Электронны лічбавы подпіс, уладальнікам асабістага ключа якога з'яўляецца фізічная асоба, лічыцца аналагам уласнаручнага подпісу. Электронны лічбавы подпіс, уладальнікам асабістага ключа якога з'яўляецца арганізацыя, можа выкарыстоўвацца:

1) у якасці аналага адбітку пячаткі арганізацыі;

2) сумесна з электронным лічбавым подпісам, уладальнікам асабістага ключа якога з'яўляецца фізічная асоба;

3) для стварэння або падпісання электронных дакументаў за пасрэдніцтвам аўтаматызаваных інфармацыйных сістэм без удзельніцтва фізічнай асобы, а таксама ў іншых выпадках, прадугледжаных заканадаўствам Рэспублікі Беларусь.

Электронны лічбавы подпіс прызначаны для засведчання інфармацыі, якая складае агульную частку электроннага дакумента, а таксама пацвярджэння цэласнасці і сапраўднасці электроннага дакумента. Можа выкарыстоўвацца і для іншых мэт, прадугледжаных заканадаўствам Рэспублікі Беларусь. Напрыклад, для падпісання электроннай копіі дакумента на папяровым носьбіце. Электронная копія дакумента на папяровым носьбіце пасля падпісання электронным лічбавым подпісам асобы, якая вырабіла гэтую электронную копію, набывае юрыдычную сілу і можа выкарыстоўвацца ў адпаведнасці з заканадаўствам Рэспублікі Беларусь.

Засведчанне інфармацыі, якая складае агульную частку электроннага дакумента, як і пацвярджэнне цэласнасці і сапраўднасці электроннага дакумента, ажыццяўляецца шляхам выкарыстання сертыфікаваных сродкаў электроннага лічбавага подпісу. Пры засведчанні інфармацыі, якая складае агульную частку электроннага дакумента, выкарыстоўваюцца асабістыя ключы арганізацыі або

фізічных асоб, якія падпісваюць электронны дакумент. Пацвярджэнне цэласнасці і сапраўднасці электроннага дакумента ажыццяўляецца з выкарыстаннем пры праверцы электроннага лічбавага подпісу адкрытых ключоў арганізацыі або фізічных асоб, якія падпісалі электронны дакумент.

Унясенне любых змяненняў у электронны дакумент пасля яго падпісання электроным лічбавым подпісам, нават выпраўленне арфаграфічных і арыфметычных памылак, робіць дакумент несапраўдным. Гэта адрознівае яго ад дакумента на папяровым носьбіце, для якога дапушчальна нанясенне розных службовых адзнак непасрэдна на сам дакумент. Такімі службовымі адзнакамі могуць быць рэгістрацыйныя індэксы, штампы, рэзалюцыі і адзнакі аб выкананні.

Электронны дакумент прыраўноўваецца да дакумента на папяровым носьбіце, які падпісаны ўласнаручна і мае аднолькавую з ім юрыдычную сілу. Электронны дакумент мае юрыдычную сілу ў тым выпадку, калі быў падпісаны:

а) у перыяд дзеяння сертыфіката адкрытага ключа незалежна ад таго, ці быў адкліканы потым адкрыты ключ, указаны ў сертыфікаце;

б) электронным лічбавым подпісам фізічнай асобы ў адпаведнасці з паўнамоцтвамі, указанымі ў атрыбутыўным сертыфікаце;

в) ад імя арганізацыі электронным лічбавым подпісам фізічнай асобы і дадаткова электронным лічбавым подпісам арганізацыі (у такім выпадку атрыбутны сертыфікат прад'яўляць не патрабуецца).

Электронны дакумент можа мець копіі. Пад копіяй электроннага дакумента разумеецца форма яго знешняй падачы на папяровым носьбіце, засведчаная вызначаным парадкам. Копію электроннага дакумента могуць засведчыць:

а) арганізацыя або індывідуальны прадпрымальнік, якія стварылі дадзены электронны дакумент;

б) арганізацыя, якая атрымала электронны дакумент ад іншай арганізацыі з дапамогай міжведамасных інфармацыйных сістэм;

в) натарыус або іншая службовая асоба, якая мае права ажыццяўляць натарыяльныя дзеянні;

г) рэгістратар арганізацыі па дзяржаўнай рэгістрацыі нерухомасці;

д) іншыя арганізацыі або фізічныя асобы ў выпадках, прадугледжаных заканадаўчымі актамі Рэспублікі Беларусь.

Закон аб электронным дакуменце і электронным лічбавым подпісе Рэспублікі Беларусь рэгламентуе парадак праверкі сапраўднасці электронных дакументаў, створаных замежнымі партнёрамі. Для гэтага прадугледжана магчымасць прызнання на тэрыторыі Рэспублікі Беларусь замежнага сертыфіката адкрытага ключа шляхам устанаўлення даверу да яго давераным трэцім бокам, які ўстанаўліваецца Прэзідэнтам Рэспублікі Беларусь.

Працэдура атрымання электроннага лічбавага подпісу і парадак яго выкарыстання. Сукупнасць працэдур, метадаў, тэхнічных, праграмных і праграмна-апаратных сродкаў, якія адносяцца да практычнага выкарыстання электроннага лічбавага подпісу, стварае тэхналогію электроннага лічбавага подпісу. Электронныя дакументы неабходна падпісваць электронным лічбавым подпісам з дзейным сертыфікатам адкрытага ключа. Каб падпісаць дакумент электронным лічбавым подпісам неабходна мець асабісты ключ электроннага лічбавага подпісу, які ўяўляе сабой паслядоўнасць сімвалаў, якая належыць канкрэтнай арганізацыі, індывідуальнаму прадпрымальніку або фізічнай асобе. Як правіла, асабісты ключ захоўваецца ў памяці камп'ютара або на здымным носьбіце інфармацыі. Асабісты ключ электроннага подпісу з'яўляецца канфідэнцыйным, уладальнік павінен захоўваць яго ў тайне і аберагаць ад змяненняў і знішчэння.

На практыцы адна і тая ж асоба можа выкарыстоўваць некалькі асабістых ключоў. Напрыклад, кіраўнік мае права атрымаць два асабістыя ключы: адзін як фізічная асоба, а другі як службовая асоба. Такія асабістыя ключы не будуць узаемазамяняльнымі, таму выкарыстаць свой электронны лічбавы подпіс фізічнай асобы для падпісання дакументаў арганізацыі кіраўнік не мае права.

Каб атрымальнік электроннага дакумента, падпісанага электронным лічбавым подпісам, мог праверыць яго верагоднасць, выкарыстоўваецца адкрыты ключ, які таксама ўяўляе паслядоўнасць сімвалаў і адпавядае канкрэтнаму асабістаму ключу. Праверка электроннага лічбавага подпісу ўяўляе сабой паслядоўнасць дзеянняў, ініцыяваных карыстальнікам адкрытага ключа, якія ажыццяўляюцца сертыфікаваным сродкам электроннага лічбавага подпісу і накіраваныя на ўстанаўленне таго, што электронны лічбавы подпіс з'яўляецца сапраўдным і пацвярджае цэласнасць электроннага дакумента.

Адкрыты ключ змяшчае і інфармацыю, якая дазваляе адназначна ідэнтыфікаваць арганізацыю, індывідуальнага прадпрымальніка або фізічную асобу, каторыя падпісалі дакумент

з дапамогай электроннага лічбавага подпісу. Адкрыты ключ даступны для любых арганізацый і фізічных асоб. Інфармацыю аб адкрытых ключах і іх уладальніках можна атрымаць праз дзяржаўную сістэму кіравання адкрытымі ключамі, напрыклад, на сайце Нацыянальнага цэнтра электронных паслуг.

У цяперашні час арганізацыяй, якая выдае ключы электроннага лічбавага подпісу, што прызнаецца ўсімі суб'ектамі гаспадарання, з'яўляецца рэспубліканскае ўнітарнае прадпрыемства "Нацыянальны цэнтр электронных паслуг". У склад гэтай арганізацыі ўваходзіць Рэспубліканскі сведчы цэнтр Дзяржаўнай сістэмы кіравання адкрытымі ключамі праверкі электроннага лічбавага подпісу Рэспублікі Беларусь, які ажыццяўляе ўсе неабходныя працэдуры, звязаныя з выдачай ключоў электронных лічбавых подпісаў.

Карпаратыўныя сістэмы могуць выкарыстоўваць ключы электроннага лічбавага подпісу, выдадзеныя ўласнымі сцвяржальнымі цэнтрамі. У якасці прыкладу можна прывесці сістэму "Кліент-банк". Атрымаць электронны лічбавы подпіс можна і ў цэнтрах рэгістрацыі рэспубліканскага ўнітарнага прадпрыемства "Інфармацыйна-выдавецкі цэнтр па падатках і зборах". Аднак такія ключы будуць прызнавацца толькі ў рамках гэтых сістэм.

Працэдура выдачы электронных лічбавых подпісаў вызначаецца рэгламентам адпаведнага цэнтра. Як правіла, такія працэдуры ідэнтычныя ва ўсіх рэгістрацыйных цэнтрах. Напрыклад, працэдура атрымання ключа электроннага подпісу ў рэгіянальных рэгістрацыйных цэнтрах рэспубліканскага сведчага цэнтра дзяржаўнай сістэмы кіравання адкрытымі ключамі наступная. Пры першым атрыманні электроннага лічбавага подпісу неабходна прайсці працэдуру рэгістрацыі абанента, пасля чаго:

1) азнаёміцца з рэгламентам рэспубліканскага сведчага цэнтра;

2) аплаціць паслугу рэспубліканскага сведчага цэнтра па рэгістрацыі з выпускам сертыфіката і выдачы носьбіта ключавой інфармацыі;

3) падрыхтаваць і падаць у рэспубліканскі сведчы цэнтр дакументы для атрымання электроннага лічбавага подпісу.

Рэспубліканскі сведчы цэнтр аказвае таксама паслугі па працягванні тэрміну дзеяння электроннага лічбавага подпісу і яго перарэгістрацыі. Перарэгістрацыя можа быць праведзена ў перыяд дзеяння электроннага лічбавага подпісу ў выпадку страты або выхаду са строю носьбіта асабістага ключа або страты паролю доступу да яго.

На практыцы часта ўзнікае пытанне, хто з супрацоўнікаў арганізацыі мае права выкарыстоўваць электронны лічбавы подпіс для падпісання дакументаў. Электронны лічбавы подпіс атрымлівае асабіста ўпаўнаважаная асоба арганізацыі, напрыклад яе кіраўнік, яго намеснік, галоўны бухгалтар. Упаўнаважаныя асобы ўказваюць пашпартныя даныя пры падачы дакументаў для атрымання электроннага лічбавага подпісу. Упаўнаважаная асоба ўказваецца таксама ў картцы і сертыфікаце адкрытага ключа электроннага лічбавага подпісу. У сувязі з гэтым падпісваць дакументы павінен той супрацоўнік, які ўказаны пры атрыманні электроннага лічбавага подпісу як упаўнаважаная асоба арганізацыі.

Выкарыстанне электроннага лічбавага подпісу неўпаўнаважаным супрацоўнікам можа выклікаць для арганізацыі і ўпаўнаважанай асобы шэраг негатыўных наступстваў. Пры падпісанні дакументаў, якія маюць памылкі або супярэчаць заканадаўству, цяжка даказаць, што электронны лічбавы подпіс прастаўлены іншай асобай. У выніку ўпаўнаважаная асоба можа быць прыцягнута да дысцыплінарнай або адміністрацыйнай адказнасці. На яе можа быць ускладзены абавязак кампенсаваць прычыненыя страты.

Неправамернай таксама з'яўляецца і перадача электроннага лічбавага подпісу іншаму супрацоўніку загадам або іншым унутраным дакументам арганізацыі. Трактаваць супрацоўніка, якому загадам перададзена права выкарыстоўваць электронны лічбавы подпіс, як прадстаўніка арганізацыі, нельга, так як прадстаўнік ставіць свой асабісты подпіс, а яго паўнамоцтвы пацвярджае даверанасць. Атрымальнікі дакументаў, падпісаных электронным лічбавым подпісам, лічаць, што дакумент падпісаны ўпаўнаважанай асобай. За дапушчаныя ў такіх дакументах памылкі і парушэнні да адказнасці прыцягваецца арганізацыя, якая з'яўляецца ўладальнікам электроннага лічбавага подпісу.

Магчыма сітуацыя, калі электронны лічбавы подпіс будзе даступны для пабочных асоб, якія не з'яўляюцца супрацоўнікамі арганізацыі. У такім выпадку незаконнае выкарыстаннае электроннага лічбавага подпісу становіцца прычынай крадзяжу грашовых сродкаў арганізацыі. Пасля звальнення супрацоўніка арганізацыі яго электронны лічбавы подпіс выкарыстоўваць нельга. Патрэбна атрымаць новы электронны лічбавы подпіс для нанава прынятага супрацоўніка, а элек-

тронны лічбавы подпіс былога супрацоўніка, каб пазбегнуць яго несанкцыянаванага выкарыстання, падлягае знішчэнню.

Такім чынам, упаўнаважанай асобе неабходна выкарыстоўваць свой электронны лічбавы подпіс асабіста, аднак яна не заўсёды мае магчымасць гэта рабіць. Упаўнаважаная асоба можа адсутнічаць па прычыне камандзіровак, водпуску, хваробы і па іншых прычынах. Выхадам з такой сітуацыі можа быць дэлегаванне паўнамоцтваў на падпісанне асобных электронных дакументаў іншым супрацоўнікам і атрыманне для кожнага з іх электроннага лічбавага подпісу. Паўнамоцтвы ўключаюцца ў службовую інструкцыю супрацоўніка або афармляюцца загадам кіраўніка, з якім супрацоўнік павінен азнаёміцца пісьмова. Такі падыход патрабуе дадатковых выдаткаў на атрыманне электроннага лічбавага подпісу, аднак ён з'яўляецца найбольш рацыянальным і бяспечным, так як дае магчымасць павысіць адказнасць супрацоўнікаў за выкарыстанне электроннага лічбавага подпісу.

Альтэрнатыўным рашэннем з'яўляецца выкарыстанне так званага мабільнага лічбавага электроннага подпісу. Ён дае магчымасць падпісваць дакументы з мабільнага тэлефона, не знаходзячыся на рабочым месцы. У мабільнага электроннага лічбавага подпісу ёсць асаблівасць, якая тычыцца захоўвання асабістага ключа, каторы захоўваецца на сім-карце. Калі электронны лічбавы подпіс мабільны, то ідэнтыфікацыя асобы і подпіс ажыццяўляюцца праз SMS. Уладальнік мабільнага электроннага лічбавага подпісу пацвярджае свае дзеянні SMS з PIN-кодам. Пры гэтым усе аперацыі абараняюцца крыптаграфічным ключом.

Атрымаць мабільны электронны лічбавы подпіс фізічныя і юрыдычныя асобы могуць у кампаніях А1 і МТС. Для атрымання мабільнага электроннага лічбавага подпісу неабходна:

1) набыць спецыяльную SIM-карту, якая падтрымлівае функцыю электроннага подпісу (SIMiD);

2) аплаціць паслугі па выдачы электроннага лічбавага подпісу;

3) мець прыстасаванні з функцыямі адпраўкі і атрымання SMS.

Адрозніваюць падпісанне электроннага дакумента і падпісанне дакумента ў электронным выглядзе. Падпісанне электроннага дакумента – гэта працэс выпрацоўкі электроннага лічбавага подпісу шляхам крыптаграфічнага пераўтварэння кантрольнай характарыстыкі агульнай часткі дакумента, які падпісваецца, з выкарыстаннем асабістага ключа асобы, якая яго падпісвае. Падпісанне дакумента ў электронным выглядзе – гэта стварэнне аналага ўласнаручнага подпісу, які ўключаецца ў дакумент у электронным выглядзе, далучаецца да яго або іншым чынам звязваецца з ім.

Сертыфікат адкрытага ключа арганізацыі або фізічнай асобы, якія падпісалі электронны дакумент, і атрыбутны сертыфікат. Як ужо было адзначана раней, адкрыты ключ выпрацоўваецца на базе асабістага ключа з выкарыстаннем сертыфікаванага сродку электроннай лічбавага подпісу. Уладальнікам адкрытага ключа з'яўляецца тая асоба, якая валодае асабістым ключом. Адкрытыя ключы праверкі электроннага лічбавага подпісу, як і асабістыя ключы, выдаюцца рэспубліканскім унітарным прадпрыемствам «Нацыянальны цэнтр электронных паслуг», у склад якога ўваходзіць Рэспубліканскі сведчы цэнтр Дзяржаўнай сістэмы кіравання адкрытымі ключамі праверкі электроннага лічбавага подпісу Рэспублікі Беларусь. Ён ажыццяўляе ўсе неабходныя працэдуры, звязаныя з выдачай адкрытых ключоў электронных лічбавых подпісаў.

Сертыфікат адкрытага ключа – гэта электронны дакумент, выдадзены сведчым цэнтрам, прызнаным ў дадзенай сістэме электроннага дакументаабароту, і змяшчае інфармацыю, якая пацвярджае прыналежнасць указанага ў ім адкрытага ключа пэўнай асобе, а таксама іншую інфармацыю, патрэбную для прызнання электроннага лічбавага подпісу сапраўдным. Калі электронны дакумент падпісаны пасля адклікання сертыфіката адкрытага ключа, то ён не можа лічыцца сапраўдным і не мае юрыдычнай сілы.

Атрыбутны сертыфікат вызначае аб'ём паўнамоцтваў фізічнай асобы і індывідуальнага прадпрымальніка па падпісанні пэўных відаў электронных дакументаў ад імя арганізацыі або фізічнай асобы, а таксама іншыя дадзеныя ім паўнамоцтвы. Пры дапамозе атрыбутнага сертыфіката арганізацыя або індывідуальны прадпрымальнік вызначаюць паўнамоцтвы фізічнай асобы, асноўным з якіх з'яўляецца падпісанне электронных дакументаў. Пры гэтым адна і тая ж фізічная асоба можа з'яўляцца ўладальнікам некалькіх атрыбутных сертыфікатаў.

Атрыбутны сертыфікат павінен змяшчаць інфармацыю: аб фізічнай асобе, якой дадзены паўнамоцтвы; арганізацыі або фізічнай асобе, ад імя якіх фізічнай асобе дадзены паўнамоцтвы; паўнамоцтвах, нададзеных фізічнай асобе ад імя арганізацыі або іншай фізічнай асобы. Уладальнік атрыбутнага сертыфікату мае права яго адклікаць. Калі адклікаецца адкрыты ключ, то гэта аўтаматычна цягне адкліканне атрыбутнага сертыфікату.

З мэтай забеспячэння праверкі электроннага лічбавага подпісу патрэбна распаўсюджванне адкрытага ключа сярод усіх зацікаўленых арганізацый і фізічных асоб. Атрыбутны сертыфікат падлягае распаўсюджванню з мэтай інфармавання ўсіх зацікаўленых асоб аб тым, хто мае права падпісваць дакументы ад імя арганізацыі. Як адкрытыя ключы, так і атрыбутныя сертыфікаты могуць распаўсюджвацца ўладальнікам адкрытага ключа або пастаўшчыком паслуг. Атрыбутны сертыфікат можа таксама распаўсюджвацца арганізацыяй або фізічнай асобай, ад імя якіх іншай фізічнай асобе надаюцца паўнамоцтвы, інфармацыя аб чым змяшчаецца ў гэтым атрыбутным сертыфікаце.

Пастаўшчыком паслуг па распаўсюджванні адкрытых ключоў з'яўляецца арганізацыя, якая можа выконваць адну або некалькі наступных функцый:

а) выданне, распаўсюджванне і захоўванне сертыфікатаў адкрытых ключоў, атрыбутных сертыфікатаў, спісаў адкліканых сертыфікатаў адкрытых ключоў і спісаў адкліканых атрыбутных сертыфікатаў;

б) верагоднае пацвярджэнне прыналежнасці адкрытага ключа пэўнай арганізацыі або фізічнай асобе;

в) выдача інфармацыі аб сапраўднасці сертыфікатаў адкрытых ключоў і атрыбутных сертыфікатаў;

г) адкліканне сертыфікатаў адкрытых ключоў і атрыбутных сертыфікатаў;

д) прастаўленне штампаў часу;

е) выпрацоўка асабістых ключоў для арганізацый або фізічных асоб.

Пастаўшчыкі паслуг ажыццяўляюць сваю дзейнасць з выкарыстаннем тэхнічных, праграмных і праграмна-апаратных сродкаў, якія адпавядаюць патрабаванням нарматыўна-прававых актаў у галіне тэхнічнага нармавання і стандартызацыі. Незалежна ад формы ўласнасці пастаўшчыкі паслуг могуць акрэдытоўвацца ў Дзяржаўнай сістэме кіравання адкрытымі ключамі.

Распаўсюджванне адкрытага ключа павінна ажыццяўляцца спосабам, які забяспечвае магчымасць доказу прыналежнасці адкрытага ключа яго ўладальніку. Распаўсюджванне адкрытых ключоў дзяржаўных органаў і іншых дзяржаўных арганізацый, а таксама атрыбутных сертыфікаў фізічных асоб, якія працуюць у такіх органах і арганізацыях, ажыццяўляецца праз дзяржаўную сістэму кіравання адкрытымі ключамі.

Заключэнне

Выкарыстанне электронных дакументаў звязана з пэўнай рызыкай, якая заключаецца ў тым, што існуе небяспека як злоўжыванняў унутры гаспадарчага суб'екта, так і махляроў, якія дзейнічаюць па-за арганізацыяй. Каб пазбегнуць страт, абумоўленых камп'ютарным махлярствам, неабходна дасканала ведаць парадак стварэння і выкарыстання ў Рэспубліцы Беларусь электронных дакументаў і электроннага лічбавага подпісу. Матэрыял артыкула дае неабходную тэарэтычную базу для авалодання такімі ведамі і выкарыстання іх у практычнай дзейнасці.

Спіс скарыстанай літаратуры

1. **Кузнецова, Т. В.** Делопроизводство. Организация и технологии документационного обеспечения управления / Т. В. Кузнецова и др. – М. : Юнити-Дана, 2015. – 359 с.

2. **О некоторых** мерах по развитию сети передачи данных в Республике Беларусь : Указ Президента Респ. Беларусь от 30 сент. 2010 г. № 515 // Консультант Плюс: Беларусь [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информации Респ. Беларусь. – Минск, 2020.

3. **Об электронном** документе и электронной цифровой подписи : Закон Респ. Беларусь от 28 дек. 2009 г. № 113-З // Консультант Плюс: Беларусь [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информации Респ. Беларусь. – Минск, 2020.

4. **Электронный** документооборот: термины и определения : приказ директора Департамента по архивам и делопроизводству М-ва юстиции Респ. Беларусь от 19 окт. 2015 г. № 39 // Консультант Плюс: Беларусь [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информации Респ. Беларусь. – Минск, 2020.

Получено 28.04.2023.