2.2. Правове регулювання електронного цифрового підпису в Україні: стан і перспективи

Основні нормативні акти, регламентуючі використання в Україні електронно-цифрового підпису, а саме Закони України «Про електронний цифровий підпис»[1] та «Про електронні документи та електронний документообіг»[2], були прийняті ще у 2003 році. Безумовно, їх прийняття мало позитивне значення й сприяло певному поширенню використання електронно-цифрового підпису, зокрема для подання податкової звітності та в банківській сфері.

Разом з тим, у сфері приватно-правових відносин електронний цифровий підпис з прийняттям указаних Законів й до цього часу не став поширеною та зручною альтернативою використання паперових документів та звичайних підписів і печаток.

З нашого погляду, такий стан речей був зумовлений, не в останню чергу, складністю адміністративних процедур, дотримання яких ви-

[1] Про електронний цифровий підпис : Закон України від 22.05.2003 № 852-IV // Голос України. – 2003. – № 119.

[2] Про електронній документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV // Голос України. – 2003. – № 119.

магалося (і вимагається) для створення та розвитку інфраструктури, необхідних для впровадження й використання системи електронних цифрових підписів.

Зазначене підтверджується й практикою. Так, згідно з відомостями центрального засвідчувального органу (Міністерства юстиції України) за 13 років з моменту прийняття Закону «Про електронний цифровий підпис» в Україні створено 38 ЦСК та АЦСК, з яких станом на середину 2016 року діє 30, серед яких 9 ЦСК та 21 АЦСК[1]. При цьому 10 з 21 АЦСК та 3 з 9 ЦСК створено органами державної влади України та державними підприємствами. Здебільшого, існуючі в Україні ЦСК та АЦСК забезпечують тільки власний документообіг.

Разом з прийняттям у 2015 році Закону України «Про електронну комерцію»[2] було створено передумови для зміни ситуації на краще, зокрема було суттєво спрощено укладання правочинів у електронній формі в галузі електронної комерції, розширено можливості прийняття (акцепту) комерційних пропозицій щодо укладання електронного правочину. Так, згідно із ч. 6 ст. 11 даного Закону, відповідь особи, якій адресована пропозиція укласти електронний договір, про її прийняття (акцепт) може бути надана шляхом:

– надсилання електронного повідомлення особі, яка зробила пропозицію укласти електронний договір, підписаного в порядку, передбаченому ст. 12 цього Закону;

– заповнення формуляра заяви (форми) про прийняття такої пропозиції в електронній формі, що підписується в порядку, передбаченому ст. 12 цього Закону;

– вчинення дій, що вважаються прийняттям пропозиції укласти електронний договір, якщо зміст таких дій чітко роз'яснено в інформаційній системі, в якій розміщено таку пропозицію, і ці роз'яснення логічно пов'язані з нею (тобто, фактично шляхом учинення конклюдентних дій).

---

[1] Електронний реєстр суб'єктів, які надають послуги, пов'язані з ЕЦП [Електронний ресурс]. – Режим доступу: http://czo.gov.ua/ca-registry.

[2] Про електронну комерцію : Закон України від 3 верес. 2015 р. № 675-VIII // Відом. Верхов. Ради України. – 2015. – № 45.

У свою чергу, відповідно до ст. 12 зазначеного Закону підписання електронного правочину пов'язується з використанням наступних засобів:

– електронного підпису або електронного цифрового підпису відповідно до Закону України «Про електронний цифровий підпис», за умови використання засобу електронного цифрового підпису всіма сторонами електронного правочину;

– електронного підпису одноразовим ідентифікатором, який являє собою дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних особою, яка прийняла пропозицію (оферту) укласти електронний договір, та надсилаються іншій стороні цього договору;

– аналога власноручного підпису (факсимільного відтворення підпису за допомогою засобів механічного або іншого копіювання, іншого аналога власноручного підпису) за письмовою згодою сторін, у якій мають міститися зразки відповідних аналогів власноручних підписів.

Разом з тим, можливість використання таких спрощених способів акцепту, як електронний підпис одноразовим ідентифікатором або аналог власноручного підпису, передбачених Законом України «Про електронну комерцію», фактично обмежена випадками укладання правочинів щодо пропонування й реалізації товарів, а також надання послуг та виконання робіт у сфері електронної комерції із використанням інформаційно-телекомунікаційних систем.

Зі сфери правового регулювання вказаного Закону виключені правочини (а) у царині надання банківських або фінансових послуг, (б) щодо об'єктів, відносно яких законом установлено спеціальний порядок переходу права власності, а також об'єктів, вилучених з цивільного обороту або обмежених у ньому, (в) стороною яких є орган державної влади або орган місцевого самоврядування в частині виконання ним функцій держави або місцевого самоврядування, (г) у сфері державних закупівель, (д) що підлягають нотаріальному посвідченню або державній реєстрації, (е) у царині сімейних правовідносин, (є) що стосуються грального бізнесу, (ж) виконання зобов'язання за якими забезпечується особою, яка уклала договір поруки або іншої форми майнового забезпечення, за умови, що вона діє

в цілях, що виходять за межі її господарської діяльності чи незалежної професійної діяльності.

Крім того, даним Законом прямо передбачено, що для можливості використання його положень до правочинів, в яких продавцем товарів, виконавцем робіт або надавачем послуг виступає фізична особа, яка не зареєстрована як фізична особа-підприємець, необхідна домовленість сторін про застосування положень цього Закону до таких правочинів.

Таким чином, прийняття вказаного Закону, на нашу думку, суттєво б спростили укладання певних цивільно-правових правочинів у галузі електронної комерції, але разом з тим, для цілого ряду випадків як і раніше вимагається використання звичайного власноручного підпису особи або електронного цифрового підпису, адже використання спрощених електронних аналогів підпису особи, встановлених Законом України «Про електронну комерцію», є неможливим.

В цілому, така позиція законодавця має свою логіку, обумовлену намаганням забезпечити належний рівень довіри в цивільному обороті. Аналіз чинного вітчизняного законодавства дає підстави вважати, що підпис особи має виконувати три основні функції: (а) фіксацію волевиявлення особи завдяки її вираженню в певній об'єктивній формі, (б) ідентифікацію підписанта за рахунок оригінальності підпису та можливості його верифікації та (в) підтвердження цілісності підписаного тексту завдяки нерозривній пов'язаності підпису із текстом. Безумовно, вказані функції повноцінно може забезпечити ЕЦП.

Для розуміння причин відносно низького поширення цього інструменту в цивільних правовідносинах, а також для визначення шляхів удосконалення правового регулювання в цій сфері видається логічним провести порівняння правового регулювання в Україні з відповідним регулюванням в ЄС, де використання ЕЦП набуло суттєво більшого поширення[1].

При цьому, вважаємо, є доцільним проведення такого порівняння за двома критеріями: (1) юридичне значення ЕЦП, й (2) вимоги до

[1] Study on the supply-side of EU e-signature market : Final Report for the DG Information Society and Media of the European Commission [Електронний ресурс] / S. Cavallini, F. Bisogni, D. Gallozzi, C. Cozza, C. Aglietti. – 2012. – С. 51. – Режим доступу: ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2141.

надання послуг ЕЦП. Зазначені критерії є основними чинниками поширення ЕЦП та легкості виходу на ринок надання послуг у цій царині, які, на нашу думку, створюють передумови для розвитку цього напрямку.

Юридичне значення електронного цифрового підпису

Україна

Відповідно до ст. 1 Закону України «Про електронний цифровий підпис»[1] електронний цифровий підпис являє собою вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується й дає змогу підтвердити його цілісність та ідентифікувати підписувача.

При цьому, відповідно до ст. 3 Закону електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

– електронний цифровий підпис 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 в сертифікаті.

Отже, в Україні ЕЦП може виступати повноцінним замінником власноручного підпису тільки у випадку, якщо використовується посилений сертифікат ЕЦП для підтвердження й перевірки такого електронного підпису.

Також не можна залишити поза увагою питання визнання сертифікатів ключів електронного цифрового підпису, виданих в інших країнах.

Статтею 6 Закону «Про електронний цифровий підпис» фактично передбачено, що в Україні визнаються електронно-цифрові підписи, виконані за допомогою лише сертифікатів ключів, одержаних тільки

[1] Про електронний цифровий підпис : Закон України від 22 трав. 2003 р. № 852-IV // Відом. Верхов. Ради України. – 2003. – № 36.

в Україні. Таким чином, учасники правовідносин у сфері електронно-цифрового підпису в Україні фактично позбавлені можливості користуватися послугами іноземних компаній, які, до речі, є світовими лідерами в цій галузі й мають розвинену інфраструктуру.

Необхідно відзначити, що положення національного законодавства в цій частині, на нашу думку, не відповідають принципам п. а) ч. 1 ст. 140 «Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони» від 27 червня 2014 р.[1], якою встановлено, що Сторони підтримують діалог з питань регулювання електронної торгівлі, що включає, inter alia, такі питання: визнання сертифікатів електронних підписів, виданих населенню, та сприяння розвитку послуг транскордонної сертифікації. При цьому, згідно з ч. 2 вказаної статті таке співробітництво може існувати у формі обміну інформацією про відповідне законодавство Сторін щодо цих питань, а також про впровадження такого законодавства.

ЄС

До 2016 року використання електронного цифрового підпису в ЄС регламентувалося Директивою ЄС «Про порядок використання електронних підписів у Європейському Співтоваристві» 1999/93/ЕС[2], яка встановлювала мінімально необхідні вимоги для використання електронних підписів у повсякденному житті.

Впровадження положень зазначеної Директиви, а також відповідних стратегій розвитку дозволило досягти таких результатів: 47% європейців користуються засобами електронних публічних послуг, 57% з яких доступні онлайн[3]. Фактично, станом на середину 2015 року, електронні публічні послуги дозволяли вирішувати в режимі онлайн такі питання повсякденного життя, як пошук роботи, освіта,

[1] Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27 червня 2014 р. // Офіц. вісн. України. – 2014. – № 75.

[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093.

[3] The State of Digital Signature in Europe [Електронний ресурс]. – Режим доступу: http://www.xnoccio.com/en/the-state-of-digital-signature-in-europe/.

заснування бізнесу, подорожі, придбання автомобілю, судове провадження за незначними позовами (наприклад, цивільне провадження за позовами з низькою ціною позову), звичайні бізнесові операції[1].

Показовим є те, що тільки 10% указаних життєвих подій можна вирішити виключно «оффлайн». Втім це було визнано недостатнім. У 2014 році було прийнято Регламент (ЄС) No 910/2014 Європейського Парламенту та Ради від 23 липня 2014 р. про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та скасування Директиви 1999/93/ЕС[2], який набрав чинності 1 липня 2016 р.

Згідно з преамбулою, основними причинами прийняття вказаного Регламенту на заміну Директиви 1999/93/ЕС було намагання підвищити рівень довіри до електронних транзакцій завдяки впровадженню загальних засад безпечних електронних операцій між громадянами, бізнесом та органами влади, що має забезпечити підвищення ефективності публічних та приватних онлайн-сервісів, електронного бізнесу й електронної комерції.

Також метою прийняття вказаного Регламенту було забезпечення наближення законодавства країн-членів ЄС у цій галузі для усунення існуючих бар'єрів транскордонного використання засобів електронної ідентифікації в країнах-членах, принаймні, для публічних сервісів. Так, ст. 6 Регламенту встановлено, що в тому випадку, якщо електронна ідентифікація з використанням засобів електронної ідентифікації та автентифікації вимагається національним законодавством чи адміністративною практикою для доступу до публічних послуг, що надаються публічним органом однієї з країн-членів, то в такій країні мають визнаватися засоби електронної ідентифікації, видані в іншій країні-члені, за умови дотримання наступних умов:

[1] EU eGovernment Report 2015 shows that online public services in Europe are smart but could be smarter [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/digital-single-market/news/eu-egovernment-report-2015-shows-online-public-services-europe-are-smart-could-be-smarter.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

– засоби електронної ідентифікації видані за схемою електронної ідентифікації, яка включена до переліку, опублікованого Європейською Комісією;

– рівень засвідчення засобу електронної ідентифікації відповідає або перевищує рівень засвідчення, який вимагається відповідним органом публічного сектору (державним, регіональним або місцевим органом влади, установою, організацією, діяльність якої регламентується нормами публічного або приватного права, уповноважена принаймні одним із таких органів влади, установою або організацією на надання публічних послуг, що діє за таким повноваженням) для доступу до публічної послуги онлайн у такій країні й за умови, що такий рівень засвідчення засобу електронної ідентифікації є суттєвим або високим;

– відповідний орган публічного сектору використовує суттєвий або високий рівень засвідчення щодо доступу до такої послуги онлайн.

При цьому, засоби електронної ідентифікації, які видані за її схемою, включеної до списку, опублікованого Європейською Комісією, та які відповідають низькому рівню засвідчення, можуть визнаватися органами публічного сектору для цілей транскордонної автентифікації для онлайн-послуг, що надаються такими органами.

З прийняттям Регламенту було розширено перелік засобів електронної ідентифікації, а також проведено їх категоризацію за рівнем засвідчення. Так, згідно зі ст. 8 Регламенту, схема електронної ідентифікації (система електронної ідентифікації, за якою засоби електронної ідентифікації надаються фізичній чи юридичній особі, або фізичній особі, яка представляє юридичну особу) має визначати низький, суттєвий та високий рівень засобу електронної ідентифікації, які, в свою чергу, мають відповідати наступним критеріям:

– низький рівень засвідчення має відноситися до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, який забезпечує обмежений рівень упевненості у заявленій або підтвердженій ідентичності особи, характеристики якого визначаються відповідними технічними специфікаціями, стандартами та процедурами, включаючи засоби технічного контролю, призначення якого полягає у зменшенні ризику зловживання або зміни ідентичності;

– суттєвий рівень засвідчення має відноситися до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, який забезпечує суттєвий рівень упевненості у заявленій або підтвердженій ідентичності особи, характеристики якого визначаються відповідними технічними специфікаціями, стандартами та процедурами, включаючи засоби технічного контролю, призначення якого полягає в суттєвому зменшенні ризику зловживання або зміни ідентичності;

– високий рівень засвідчення має відноситися до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, який забезпечує більш високий рівень упевненості у заявленій або підтвердженій ідентичності особи, характеристики якого визначаються відповідними технічними специфікаціями, стандартами та процедурами, включаючи засоби технічного контролю, призначення якого полягає в запобіганні зловживанню або зміні ідентичності.

Регламентом виокремлено три види електронного підпису:

– електронний підпис – дані в електронній формі, які додані або логічно пов'язані іншими відомостями в електронній формі та які використовуються підписантом для підпису;

– покращений електронний підпис – електронний підпис, який відповідає наступним вимогам: (a) унікально пов'язаний з підписантом; (b) здатен ідентифікувати підписанта; (c) створений з використанням відомостей для створення електронного підпису, які з високим рівнем надійності перебувають під особистим контролем підписанта; та (d) пов'язаний з інформацією, для підписання якої цей підпис використовується, таким чином, щоб можна було встановити всі наступні зміни в такій інформації;

– кваліфікований електронний підпис – покращений електронний підпис, який створено кваліфікованим засобом створення електронного підпису та який базується на кваліфікованому сертифікаті для електронних підписів.

Юридичне значення використання електронного підпису визначається ст. 25 Регламенту, відповідно до якої юридичне значення електронного підпису як допустимого доказу в юридичних провадженнях не повинно заперечуватися виключно на тих підставах, що він існує в електронній формі або що він не відповідає вимогам ква-

ліфікованого електронного підпису. При цьому, останній має юридичне значення власноручного підпису.

На відміну від України, Регламент ЄС прямо передбачає обов'язкове визнання кваліфікованих електронних підписів, основаних на кваліфікованому сертифікаті, виданому в будь-якій іншій країні ЄС: відповідно до ст. 25 Регламенту, кваліфікований електронний підпис, оснований на кваліфікованому сертифікаті, що виданий в одній країні-члені ЄС повинен визнаватися кваліфікованим електронним підписом у всіх інших країнах-членах.

Крім того, Регламентом було введено категорію електронної печатки для використання в наданні публічних послуг, визначено порядок та юридичні наслідки її використання.

Електронна печатка являє дані в електронній формі, які додаються або логічно пов'язані з іншими даними в електронній формі та яка забезпечує підтвердження походження і цілісність інформації.

Покращена електронна печатка являє собою електронну печатку, яка відповідає наступним вимогам: (a) унікально пов'язана з юридичною особою, яка створила печатку; (b) здатна ідентифікувати створювача печатки; (c) створена з використанням відомостей для створення електронної печатки, які з високим рівнем надійності перебувають під особистим контролем створювача печатки; та (d) пов'язана з інформацією, до якої вона відноситься, таким чином, щоб можна було встановити всі наступні зміни в такій інформації.

В свою чергу, кваліфікована електронна печатка являє собою електронну печатку, яка створена з використанням пристрою створення кваліфікованих електронних печаток та основана на кваліфікованому сертифікаті для електронних печаток.

Аналогічно електронному підпису, правові наслідки використання електронної печатки не можуть бути відхилені тільки на тій підставі, що вона втілена в електронній формі або не відповідає вимогам до кваліфікованих електронних печаток.

Регламентом також передбачається, що кваліфікована електронна печатка задовольняє презумпції цілісності інформації й коректності її походження, до якої вона додана. При цьому, як і у випадку з кваліфікованим електронним підписом, кваліфікована електронна печат-

ка, основана на кваліфікованому сертифікаті, виданому в одній країні-члені ЄС, має визнаватися в такій якості й у інших країнах-членах.

Як слідує з Регламенту, основним призначенням електронної печатки є її використання при наданні публічних послуг.

Крім того, Регламентом запроваджено такі інструменти, як електронний штамп часу, служби електронної зареєстрованої доставки та автентифікації сайту Інтернет.

Так, електронний штамп часу забезпечує підтвердження точності часу та дати, а також цілісність даних, з якими пов'язаний такий час та дата. Служба електронної зареєстрованої доставки має слугувати підтвердженням презумпцію цілісності інформації, відправленої ідентифікованим відправником, її одержання ідентифікованим адресатом та точність дати та часу відправки й одержання. У свою чергу, сертифікат автентифікації інтернет-сайту має забезпечувати підтвердження автентифікації інтернет-сайту та його зв'язок з фізичною чи юридичною особою, якій видано відповідний сертифікат.

По-суті, указаний Регламент покликаний закласти підвалини створення єдиного цифрового ринку та електронного урядування для всіх громадян країн-членів за допомогою широкого використання електронних підписів, які стають критично важливим елементом для розвитку.

Вимоги для надання послуг електронного цифрового підпису

Україна

Чинне законодавство України містить диференційовані детальні вимоги до учасників приватноправових відносин, які забезпечують обіг електронних цифрових підписів, а саме: центрів сертифікації ключів (надалі – ЦСК) та акредитованих центрів сертифікації ключів (надалі – АЦСК).

Аналіз Закону України «Про електронний цифровий підпис» дозволяє сформулювати наступні основні відмінності ЦСК від АЦСК:

– ЦСК може надавати послуги електронного цифрового підпису та обслуговувати звичайні сертифікати ключів (ст. 8);

– АЦСК може надавати послуги електронного цифрового підпису та обслуговувати виключно посилені сертифікати ключів (ч. 2 ст. 9);

– АЦСК має виконувати всі зобов'язання та вимоги, встановлені законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати для надання послуг електронного цифрового підпису надійні засоби електронного цифрового підпису (ч. 3 ст. 9). Під надійним засобом електронного цифрового підпису розуміється засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації (абз. 14 ч. 1 ст. 1).

Практично ця різниця полягає у рівні захищеності ЕЦП, що обумовлює, зокрема, можливі сфери використання ЕЦП. Так, приміром, надання послуг електронного цифрового підпису в правовідносинах, суб'єктом яких є орган державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності можливе тільки з використанням посилених сертифікатів (постанова Кабінету Міністрів України «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» від 28 жовтня 2004 р. за № 1452)[1].

Розглянемо детальніше нормативне регулювання вимоги щодо створення та діяльності ЦСК та АЦСК.

Аналіз чинного вітчизняного законодавства в цій сфері дозволяє зробити висновок, що до створення та діяльності ЦСК та АЦСК в Україні пред'являються численні вимоги, зокрема організаційні й кваліфікаційні, вимоги щодо захисту інформації, технологічні тощо. При цьому, з огляду на те, що багато з цих вимог мають суто технічний характер і визначаються не зареєстрованими в Міністерстві юстиції України актами, навіть складення повного корпусу нормативних документів у цій галузі викликає певні труднощі.

Загальні вимоги до створення та діяльності ЦСК та АЦСК визначаються Законами України «Про електронний цифровий підпис»,

[1] Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності : постанова Каб. Міністрів України від 28.10.2004 № 1452 // Уряд. кур'єр. – 2004. – № 214.

«Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах»[1] тощо.

В якості ЦСК може виступати юридична особа будь-якої організаційно-правової форми або приватний підприємець-фізична особа, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі органу виконавчої влади або іншого державного органу (ч. 1 ст. 8 Закону України «Про електронний цифровий підпис»). Відповідно до постанови Кабінету Міністрів України «Про затвердження Положення про центральний засвідчувальний орган» від 28 жовтня 2004 р., №1451[2], виконання функцій центрального засвідчувального органу покладено на Міністерство юстиції України.

Протягом здійснення своєї діяльності ЦСК зобов'язаний забезпечувати захист інформації в автоматизованих системах відповідно до законодавства. Фактично йдеться про дотримання вимог до захисту інформації в автоматизованих системах. Вимоги до такого захисту інформації встановлені Законом України «Про захист інформації в інформаційно-телекомунікаційних системах»[3] та «Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених постановою Кабінету Міністрів України №373 від 29 березня 2006 р.[4]

Відповідно до ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» державні інформаційні

[1] Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 №80/94-ВР : в ред. Закону України «Про внесення змін до Закону України "Про захист інформації в автоматизованих системах"» від 31.05.2005 №2594-IV // Голос України. – 2005. – №116.

[2] Про затвердження Положення про центральний засвідчувальний орган : постанова Каб. Міністрів України від 28 жовт. 2004 р. №1451 // Уряд. кур'єр. – 2004. – №214.

[3] Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 1994 р. №80/94-ВР : в ред. Закону України «Про внесення змін до Закону України "Про захист інформації в автоматизованих системах"» від 31 трав. 2005 р. №2594-IV // Голос України. – 2005. – №116.

[4] Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Каб. Міністрів України від 29 берез. 2006 р. №373 // Уряд. кур'єр. – 2006. – №73–74.

ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Таке підтвердження здійснюється за результатами державної експертизи в порядку, встановленому законодавством. При цьому, для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації.

Таким чином, законодавством прямо передбачаються вимоги щодо забезпечення захисту інформації в ході діяльності ЦСК. Такий захист має забезпечуватися дотриманням організаційних і технічних вимог діяльності, а також створенням комплексної системи захисту інформації (далі – КСЗІ). Детально порядок створення такої КСЗІ регламентується зазначеними вище Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та низкою нормативних документів Державної служби технічного захисту інформації Служби безпеки України.

Відповідно до п. 16 вказаних Правил комплексна система захисту інформації призначається для захисту інформації від (а) витоку технічними каналами; (б) несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів; (в) спеціального впливу на засоби обробки інформації.

Захист інформації від витоку технічними каналами та її убезпечення від спеціального впливу мають забезпечуватися в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації.

Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, має забезпечуватися в усіх системах.

Детальні технічні та організаційні вимоги до створення комплексної системи захисту інформації встановлені низкою підзаконних нормативних актів, зокрема, незареєстрованим у Міністерстві юсти-

ції України Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України №22 від 28 квітня 1999 р., яким затверджені:

– «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1.-002-99»[1];

– «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99»[2];

– «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99»[3];

– «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. НД ТЗІ 3.7-001-99»[4].

Створення такої системи передбачає формування технічного завдання, обумовленого особливостями діяльності об'єкта, власне розробку такої комплексної системи уповноваженим суб'єктом, її впровадження та наступну державну експертизу.

---

[1] Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1.-002-99 [Електронний ресурс] : затв. наказом Департаменту спеціал. телекомунікац. систем та захисту інформації Служби безпеки України від 28 квіт. 1999 р. №22. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document;jsessionid=E7C5D8587677D262947BF00EF44548E6.app1?id=106340.

[2] Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 [Електронний ресурс] : затв. наказом Департаменту спеціал. телекомунікац. систем та захисту інформації Служби безпеки України від 28 квіт. 1999 р. №22. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=E7C5D8587677D262947BF00EF44548E6.app1?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343.

[3] Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99 [Електронний ресурс] : затв. наказом Департаменту спеціал. телекомунікац. систем та захисту інформації Служби безпеки України від 28 квіт. 1999 р. №22. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document;jsessionid=E7C5D8587677D262947BF00EF44548E6.app1?id=106342.

[4] Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. НД ТЗІ 3.7-001-99 [Електронний ресурс] : затв. наказом Департаменту спеціал. телекомунікац. систем та захисту інформації Служби безпеки України від 28 квіт. 1999 р. №22. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document;jsessionid=E7C5D8587677D262947BF00EF44548E6.app1?id=106349.

Державна експертиза комплексної системи захисту інформації в ІТС провадиться згідно з Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 р. за № 93[1] та «Порядком проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 2.6-001-11», затвердженим наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 25 березня 2011 р., № 65[2].

Таким чином, створення в Україні навіть простого ЦСК потребує проходження складних та тривалих процедур.

У випадку ж створення й діяльності АЦСК ситуація є набагато складнішою, оскільки діяльність такого центру потребує акредитацій. Основні вимоги до АЦСК та порядок проходження акредитації визначаються «Порядком акредитації центру сертифікації ключів», затвердженим постановою Кабінету Міністрів України № 903 від 13 липня 2004 р.[3] Крім того, у своїй діяльності АЦСК має дотримуватися вимог Правил посиленої сертифікації, затвердженими Наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 січня 2005 року № 3[4].

---

[1] Про затвердження Положення про державну експертизу в сфері технічного захисту інформації : наказ Адмін. Держ. служби спеціал. зв'язку та захисту інформації України від 16 трав. 2007 р. № 93 // Офіц. вісн. України. – 2007. – № 52.

[2] Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 2.6-001-11 [Електронний ресурс] : затв. наказом Адмін. Держ. служби спеціал. зв'язку та захисту інформації України від 25 берез. 2011 р. № 65. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/doccatalog/document;jsessionid=E7C5D8587677D262947BF00EF44548E6.app1?id=106345.

[3] Про затвердження Порядку акредитації центру сертифікації ключів : постанова Каб. Міністрів України від 13 лип. 2004 р. № 903 // Уряд. кур'єр. – 2004. – 15 верес. (№ 173).

[4] Про затвердження Правил посиленої сертифікації : наказ Департаменту спеціал. телекомунікац. систем та захисту інформації Служби безпеки України від 13 січ. 2005 р. № 3 // Офіц. вісн. України. – 2005. – № 5.

Умовно такі вимоги можна розділити на наступні категорії:

– вимоги до програмно-технічного комплексу: (а) до криптографічного захисту інформації. Зокрема, вимагається мати сертифікати відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації; (б) до технічного захисту інформації, зокрема вимагається мати сертифікати відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації; (в) до створення та атестації відповідності комплексної системи захисту інформації, якими визначено необхідність створення такої системи та проходження державної атестації;

– вимоги до спеціальних приміщень, які детально прописані в Правилах посиленої сертифікації;

– вимоги до внутрішніх регламентів та правил роботи центру, які включають у себе наявність: (а) Регламенту роботи центру, зміст якого має відповідати вимогам Правил посиленої сертифікації, (б) Положення, яким визначаються посадові обов'язки, кваліфікаційні вимоги та відповідальність посадових осіб центру сертифікації ключів, (в) Положення про службу захисту інформації центру сертифікації ключів, (г) Плану-схеми приміщень центру сертифікації ключів та порядку доступу до спеціальних приміщень, (д) Порядку зберігання окремих резервних копій посилених сертифікатів ключів та списків відкликаних сертифікатів, сформованих акредитованим центром; (е) Порядку синхронізації з Всесвітнім координованим часом (UTC).

Крім того, до проведення акредитації ЦСК зобов'язаний внести на спеціальний рахунок, відкритий у банківській установі, кошти в розмірі стократної мінімальної заробітної плати для забезпечення відшкодування збитків, які можуть бути завдані підписувачам, користувачам або третім особам унаслідок неналежного виконання акредитованим центром своїх зобов'язань.

Після своєї акредитації АЦСК у своїй діяльності повинен забезпечувати дотримання політики сертифікації, яка включає в себе організаційні, технічні й технологічні умови діяльності акредитованих центрів під час обслуговування ними сертифікатів. З огляду на суто технічний характер та казуїстичність зазначених вимог не вбачається

доцільним наводити повністю, із ними можна ознайомитися в Правилах посиленої сертифікації.

Таким чином, створення та діяльність ЦСК і АСЦК в України є непрозорим, оскільки регламентується численними неупорядкованими нормами, часто встановленими навіть незареєстрованими в Міністерстві юстиції України нормативними актами. При цьому технічні регламенти визначаються нормативними документами, створеними ще в 1999 р., а певні технічні стандарти визначаються ГОСТами часів СРСР. Зрозуміло, що питання узгодження таких стандартів із запровадженими в ЄС сучасними технічними стандартами взагалі залишається за кадром.

ЄС

Директива ЄС 1999/93/ЕС містила нечисленні чітко визначені технічні вимоги, які стосувалися лише провайдерів послуг посилених сертифікатів ключів, які використовувалися в сфері публічно-правових відносин, зокрема, при сплаті податків, у банківській сфері тощо. Регламентування ж використання електронного цифрового підпису в приватноправових відносинах було залишено учасникам таких відносин.

Так, одним із основних принципів організації ринку електронних цифрових підписів в ЄС було закріплення в п. 12 Преамбули Директиви 1999/93/ЕС можливості надання послуг електронного цифрового підпису особами як публічного, так і приватного права. При цьому країни ЄС зобов'язалися не забороняти провайдерам послуг у сфері електронного цифрового підпису вільно без обмежень використовувати власні схеми акредитації. Також країни ЄС зобов'язалися не вводити обмеження щодо таких схем акредитації, які могли б обмежити конкуренцію в цій сфері.

Таким чином, в ЄС використання електронних цифрових підписів здійснювалося здебільшого за диспозитивним принципом, а регулююче втручання держав-учасниць було обмежено. Такий підхід, безумовно, сприяв розвитку цих відносин на певному етапі.

Ситуація дещо змінилася з набуттям чинності Регламенту ЄС 910/2014, зокрема були введені детальні й диференційовані вимоги до провайдерів довірчих послуг. Так, відповідно до ст. 19 Регламенту, кваліфіковані та некваліфіковані провайдери довірчих послуг

зобов'язані вживати необхідні технічні й організаційні заходи з метою управління ризиками, пов'язаними з безпекою тих довірчих послуг, які вони надають, за принципом співмірності рівня безпеки ступеню ризику.

При цьому Регламентом визначаються лише загальні засади створення та діяльності кваліфікованих провайдерів довірчих послуг. Діяльність інших провайдерів довірчих послуг, а також нагляд за їх діяльністю здійснюється за принципом «легкого торгання»: держава втручається в їх діяльність тільки у випадку виникнення проблем і скарг. В інших же випадках усе відбувається за диспозитивним принципом і регулюється ринком. Безумовно, це створює передумови для легкості виходу на ринок надання цих послуг і його розвитку.

Для можливості надання кваліфікованих довірчих послуг провайдер послуг довіри, який не має кваліфікованого статусу зобов'язаний подати до наглядового органу повідомлення про свої наміри надавати такі послуги разом зі звітом про відповідність, виданим органом підтвердження відповідності. Після цього, надані заявником відомості підлягають перевірці контролюючим органом, за наслідками якої, у випадку відповідності провайдера довірчих послуг установленим вимогам, йому надається кваліфікований статус і він вноситься до загальнодоступного списку кваліфікованих провайдерів довірчих послуг.

Після внесення кваліфікованого провайдера довірчих послуг до списку таких провайдерів, він одержує право надавати кваліфіковані довірчі послуги й має право використовувати знак довіри ЄС для позначення простоти, визнаності та прозорого характеру довірчих послуг, які він надає.

Крім того, протягом своєї діяльності кваліфікований провайдер довірчих послуг відповідно до ст. 24 Регламенту зобов'язаний проходити аудит кожні 24 місяці, метою чого є підтвердження відповідності такого провайдера та його послуг нормативним вимогам.

Організаційні вимоги до діяльності провайдера кваліфікованих довірчих послуг визначаються Регламентом і включають у себе вимоги щодо порядку видачі кваліфікованих сертифікатів, порядок ідентифікації осіб, які звернулися за одержанням такого сертифікату, порядок повідомлення наглядового органу про зміни у своїй діяль-

ності, порядок інформування замовників про свої послуги, забезпечувати страхове покриття своєї відповідальності, а також інші вимоги щодо його діяльності, зокрема, використовувати надійні системи та продукти для забезпечення безпеки й зберігання інформації, а також вживати необхідних заходів для забезпечення такої безпеки.

Крім того, Регламентом визначені загальні вимоги до кваліфікованих сертифікатів електронних підписів, електронних печаток, автентифікації інтернет-сайтів, а також до пристроїв створення кваліфікованих електронних підписів.

Детальні вимоги до організації діяльності кваліфікованих провайдерів довірчих послуг визначаються відповідними Регламентами імплементації, прийнятими Європейською комісією, зокрема:

– Регламентом імплементації Європейської комісії 2015/1502 від 8 вересня 2015 р. про встановлення мінімальних технічних специфікацій і процедур для рівнів засвідчення засобів електронної ідентифікації[1], яким визначаються організаційні вимоги щодо забезпечення відповідного рівня засвідчення (звичайний, суттєвий, високий);

– Регламентом імплементації Європейської комісії 2016/650 від 25 квітня 2016 р. про визначення стандартів оцінки безпеки пристроїв створення кваліфікованих підписів і печаток[2], яким чітко визначається перелік відповідних стандартів ISO та EN, які мають застосовуватися.

Вимоги до алгоритмів, які мають використовуватися у кваліфікованому електронному підписі, визначаються Рішенням імплементації Європейської комісії 2015/1506 від 8 вересня 2015 р. про встановлен-

[1] Commission implementing regulation 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1467895827146&uri=CELEX:32015R1502.

[2] Commission implementing regulation 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1467895827146&uri=CELEX:32016D0650.

ня специфікацій, що відносяться до формату покращених електронних підписів та електронних печаток для їх визнання органами публічного сектору[1].

В цілому, всі технічні вимоги, які стосуються діяльності провайдерів довірчих послуг зумовлені здебільшого міркуваннями забезпечення інтероперабельності засобів електронної ідентифікації між країнами-членами ЄС.

Таким чином, регламентування створення й діяльності провайдерів довірчих послуг здійснюється прозоро, а втручання держави є мінімально необхідним для забезпечення створення Єдиного цифрового ринку для всіх громадян ЄС.

Підводячи підсумки, слід зазначити, що вимоги українського законодавства до створення та діяльності ЦСК та АЦСК, на нашу думку є занадто надмірними порівняно з Європейським Союзом. Крім того, на відміну від ЄС, вимоги вітчизняного законодавства щодо створення та діяльності центрів сертифікації ключів викладені здебільшого у бланкетних та відсилочних нормах цілого ряду нормативних актів, які навіть не були зареєстровані Міністерством юстиції України. Все це дає підстави вважати, що існуюча в Україні нормативно-правова база суттєво стримує розвиток відповідних суспільних відносин у цій галузі.

На нашу думку, вказані недоліки не можуть бути виправлені внесенням окремих косметичних змін до актів чинного законодавства України. Найбільш оптимальним виходом із цієї ситуації було б узгодження національного законодавства із Регламентом Європейського Парламенту та Ради від 23 липня 2014 р., № 910/2014 про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та скасування Директиви 1999/93/ЕС з метою суттєвого спрощення відповідних адміністративних процедур.

Такий підхід, вважаємо, забезпечить розвиток відносин у цій сфері, імплементацію вже існуючого успішного досвіду розвитку

[1] Commission implementing decision 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015D1506.

ринку надання послуг електронного цифрового підпису, а також створення підґрунтя для впровадження засобів функціонування інформаційного суспільства.

Необхідно відзначити, що робота в цьому напрямку вже ведеться. Так, 17 травня 2016 р. до Верховної Ради України було подано проект Закону «Про електронні довірчі послуги»[1], спрямований на гармонізацію національного законодавства України з положеннями Регламенту (ЕС) № 910/2014 від 23 липня 2014 р. про електронну ідентифікацію та довірчі послуги для електронних транзакцій[2]. Більше того, положення Регламенту й були взяті за основу при розробці вказаного проекту Закону.

Проект містить численні позитивні зміни, а саме: (а) закріплення принципу інтероперабельності, (б) можливість визнання іноземних довірчих послуг, (в) визначення рівнів електронної ідентифікації, (г) задоволення потреб осіб з обмеженими можливостями, тощо.

Переконані, що в даному випадку слід рухатися далі й на законодавчому рівні узгодити технічні вимоги до операторів довірчих послуг з відповідними стандартами ЄС. З нашої точки зору, це могло б суттєво сприяти розвитку ринку надання цих послуг, а також забезпечувало б сумісність із засобами електронної автентифікації ЄС.

---

[1] Про електронні довірчі послуги [Електронний ресурс] : Проект Закону України № 4685. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=59139&pf35401=388068.

[2] Гадомський Д. В законопроекте № 4685 почти весь текст регламента ЕС об электронной идентификации и доверительных услугах [Електронний ресурс] / Д. В. Гадомський // Юрид. практика. – Режим доступу: http://pravo.ua/news.php?id=0054936.