

ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ ОСОБИ В УМОВАХ ВОЄННОГО СТАНУ З ВИКОРИСТАННЯМ УДОСКОНАЛЕНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ (КЕП, SMART-ID, MOBILE ID)

ELECTRONIC PERSONAL IDENTIFICATION IN THE CONDITIONS OF MARITAL STATE USING ADVANCED DIGITAL TECHNOLOGIES (KEP, SMART-ID, MOBILE ID)

Шумак І.О., к.ю.н.,
доцент кафедри інтелектуальної власності та приватного права
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Царик О. В., студентка III курсу юридичного факультету
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Наукове дослідження присвячено визначенню способів та можливостей безпечної та захищеної електронної ідентифікації особи з використанням кваліфікованого електронного підпису, його вдосконаленої форми SmartID, мобільного цифрового підпису (Mobile ID) в сучасних цивільно-правових відносинах. Досліджено правовий режим електронного цифрового підпису, кваліфікованого електронного підпису (далі – КЕП) в законодавстві, використання останнього при укладанні правочинів, технологію використання мобільного цифрового підпису (Mobile ID) в цивільному обороті, забезпечення захисту приватних даних фізичних чи юридичних осіб. Засоби електронної ідентифікації особи, такі як кваліфікований електронний підпис (КЕП) та мобільний цифровий підпис (Mobile ID) допомагають забезпечити безпечну ідентифікацію особи. Ці технології використовуються для захисту персональних даних під час використання цивільно-правових договорів.

Проаналізовано укладання окремих видів договорів в умовах воєнного стану з урахуванням можливості захисту персональних даних з використанням кваліфікованого електронного підпису, мобільного цифрового підпису. Запропоновано запровадження інструментів електронної ідентифікації, постійний моніторинг з боку держави у сфері Mobile ID задля поширення можливості безпечно використання електронного цифрового підпису для укладання цивільно-правових договорів. Також було досліджено процес реалізації права на приватність життя та на повагу до останнього з метою укладення належних правочинів та надання послуг, захищаючи при цьому конфіденційну інформацію особи. Було визначено як забезпечення приватності реалізовано у електронних цифрових технологіях (КЕП, Smart-id, Mobile id). Встановлено можливі проблеми, які виникають на даному етапі застосування цих технологій та способи їх подолання.

Ключові слова: воєнний стан, електронна ідентифікація, електронний підпис, персональні дані, захист даних.

The scientific research is devoted to determining the methods and possibilities of safe and secure electronic identification of a person using a qualified electronic signature, its improved form SmartID, mobile digital signature (Mobile ID) in modern civil legal relations. The legal regime of electronic digital signature, qualified electronic signature (hereinafter – KEP) in the legislation, the use of the latter in concluding transactions, the technology of using a mobile digital signature (Mobile ID) in civil transactions, ensuring the protection of private data of individuals or legal entities have been studied. Means of electronic identification of a person, such as a qualified electronic signature (KEP) and a mobile digital signature (Mobile ID) help ensure secure identification of a person. These technologies are used to protect personal data when using civil law contracts.

The conclusion of certain types of contracts in the conditions of martial law was analyzed, taking into account the possibility of protecting personal data using a qualified electronic signature, a mobile digital signature. It is proposed to introduce electronic identification tools, constant monitoring by the state in the field of Mobile ID in order to spread the possibility of safe use of electronic digital signature for concluding civil law contracts. The process of realizing the right to privacy of life and respect for the latter was also investigated in order to conclude appropriate transactions and provide services, while protecting confidential personal information. It was determined how to ensure privacy implemented in electronic digital technologies (KEP, Smart-id, Mobile id). Possible problems that arise at this stage of the application of these technologies and ways to overcome them have been identified.

Key words: martial law, electronic identification, electronic signature, personal data, data protection.

Постановка проблеми. Внаслідок збройної агресії РФ проти України та стрімкого впливу інформаційно-комунікаційних технологій на товарно-грошові відносини, що знаходяться у сфері цивільного обороту в Україні, суттєво зростає кількість договорів, які укладаються в електронній формі. Сфера застосування електронних документів як у договірних цивільних правовідносинах, так і в цілому у відносинах приватних осіб з державними органами, судами та з іншими суб'єктами публічного права, має очевидну тенденцію до розширення і зростання. У багатьох сферах товарно-грошового обміну взаємодія виконавців і замовників вийшла на абсолютно новий організаційно-правовий рівень та здійснюється виключно в онлайн режимі. Через територіальну віддаленість багатьох українців та компаній внаслідок воєнних дій на території держави, співпраця з іноземними компаніями та партнерами, надання послуг громадянам іншої держави не завжди відбувається підписанням досягнутої домовленості на паперових носіях. Актуальними та важливими є питання

забезпечення при укладанні таких договорів захисту персональних даних осіб, налагодження системи її гарантування на законодавчому рівні та реалізації останньої в умовах воєнного стану.

Аналіз останніх досліджень і публікацій. Створення, особливості застосування та отримання електронного підпису досліджували, зокрема, М. Білуха, Т. Мельник, В. Онищенко. Правове регулювання електронно-цифрового підпису, як засобу захисту електронних документів, визначення його ознак та функцій, розглядали у своїх працях: Н. Варновський, В. Глушков, М. Денісова, В. Колісник, Г. Купріянова, А. Матвієнко, М. Цивін, В. Ященко та ін.

Виклад основного матеріалу. З огляду на стрімкі тенденції діджиталізації сучасного життя та активний розвиток цифрових технологій, серйозних змін зазнають сучасні правові відносини. Внаслідок збройної агресії РФ проти України гостро постало питання про необхідність забезпечення застосування нових електронно-цифрових технологій для вчинення правочинів, забезпечення судо-

вого захисту, доступу до інформаційних систем. Існує потреба у належному більш чіткому врегулюванні таких процесів та гарантування всебічного захисту інтересів учасників правовідносин та їх даних.

У XXI ст. інформаційно-комунікаційні технології стали провідною рушійною силою, яка досить потужно впливає на всі сфери життя суспільства та здатна забезпечити їх належне існування у сучасних умовах. На сьогодні в Україні істотно відчувається потреба в унормуванні нових відносин, що виникають внаслідок постійного розвитку комп'ютерних технологій.

Розвиток і удосконалення електронного документообігу та комерції в Україні стикається з недосконалістю окремих питань правового регулювання щодо електронного цифрового підпису і електронного документообігу. Тому впровадження нових технологій дає шанс, що нові позитивні зміни отримають своє відповідне нормативно-правове закріплення, у тому числі у сфері діджиталізації.

Відповідно до ст. 205 Цивільного кодексу України правочин може вчинятись усно або в письмовій формі. Якщо правочин підписаний його сторонами, він є вчиненим у письмовій формі. Якщо зміст правочину зафіксований в одному чи декількох документах (електронних в тому числі), він вважається таким, що вчинений у письмовій формі. Виходячи з положень ч. 3 ст. 207 Цивільного кодексу України про можливість вчинення підпису за допомогою електронного підпису, цей правочин вважається різновидом письмової форми правочину [1].

Згідно із Законом України «Про електронні документи та електронний документообіг» завершенням оформлення електронного документу є вчинення електронного підпису. Законодавче визначення електронного підпису містить ст. 1 Закону України «Про електронні довірчі послуги» – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних. Під поняттям «кваліфікований електронний підпис» розуміють удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа [2; 3].

КЕП, який було запроваджено Законом України «Про електронні довірчі послуги», складається з більш захищеного варіанту ключа [3]. Як наслідок, кваліфіковані надавачі електронних послуг були зобов'язані забезпечити дотримання нових стандартів та розпочати випуск та підтримку КЕП замість ЕЦП. Відтак, з введенням КЕП з'явилась можливість захистити своє право на приватність та мінімізувати його порушення.

Право на приватність передбачено ст. 8 європейської Конвенції про захист прав людини і основоположних свобод, в якій зазначається, що кожна особа має право на повагу до власного приватного та сімейного життя, житла та кореспонденції.

Відповідні положення цієї Конвенції відображено в Конституції України, зокрема у ст. 28, яка передбачає собою певні аспекти фізичної приватності (жодна людина без вільної згоди не може бути піддана медичним, науковим чи іншим дослідженням); ст. 30 (забороняється та не допускається проникнення у житло чи володіння іншої особи); ст. 31 щодо захисту комунікаційної сфери, як таємниці листування, телефонних розмов тощо; ст. 32 захищає інформаційну приватність (не допускається втручання в особисте та сімейне життя, збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди) [4].

Поняття приватності (прайвесі) є доволі широким, до якого входять такі складові, як право на ім'я, на особистий розвиток, релігійні і особисті переконання, гендерна ідентичність; захист даних та особистої інформації, відомостей про здоров'я, охорона шлюбно-сімейних відносин тощо.

Зокрема, Закон України «Про захист персональних даних» передбачає, що персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Відповідно до ч. 2 ст. 24 цього закону передбачено, що в органах державної влади, органах місцевого самоврядування, а також у володільців чи розпорядників персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Вважаємо, що КЕП забезпечує приватність особи, оскільки зберігається на захищеному носії інформації з криптографічним захистом, що гарантує існування КЕП лише у єдиному екземплярі та, відповідно, виконання усіх операцій всередині такого носія. Крім цього останній забезпечує невилучення секретного ключа КЕП і є захищеним паролем доступу для запобігання несанкціонованому використанню в разі втрати носія. Використання такого засобу вберігає підпис від копіювання та гарантує, що сторонній особі витягнути секретний ключ з захищеного носія неможливо.

Недоліком, на наш погляд, є те, що в умовах воєнного стану звернутися до кваліфікованих надавачів електронних послуг для отримання КЕП чи його продовження для багатьох громадян України є складним процесом. В основному це питання вирішено у Постанові Кабінету Міністрів України № 617 «Про внесення змін до постанови Кабінету Міністрів України від 17 березня 2022 р. № 300» про подовження терміну дії електронного підпису. Міністерство цифрової трансформації України разом з Державною службою спеціального зв'язку та захисту інформації України уповноважені забезпечити безперебійне функціонування системи надання е-послуг та можуть на основі раніше створених ключів самостійно сформувати новий КЕП [5].

Для підтвердження чинності відкритого ключа такі колективні суб'єкти, як органи державної влади, органи місцевого самоврядування, установи, організації та підприємства державної форми власності, а також індивідуальні – нотаріуси, державні реєстратори тощо, використовують лише кваліфікований сертифікат відкритого ключа. Зокрема, для реалізації та виконання повноважень, які спрямовані на набуття, припинення чи зміну прав та/або обов'язків юридичної або фізичної особи, використовують лише засоби кваліфікованого електронного підпису чи печатки [6].

Проте для забезпечення належного функціонування електронних підписів необхідно провести низку технологічних вдосколень таким чином, щоб кожна особа, могла здійснювати правочини онлайн безпечно й конфіденційно та, при цьому, щоб не порушувались основоположні права останньої.

Що стосується технології SmartID, вона також передбачає собою процедуру кваліфікованого електронного підпису, який є аналогом власноручного підпису. Кваліфікований електронний підпис SmartID було запроваджено Приватбанком України, який з часом почав набирати все більшого поширення та популярності (наприклад, схожа система передбачена у застосунку Дія. Підпис). Відмінність SmartID від звичайного КЕП полягає в тому, що він зберігається в хмарному середовищі та приєднаний до гаджету особи, де, наприклад, встановлено мобільний додаток «Приват24 для бізнесу». Також технологія SmartID більш зручна, на відміну від КЕП, процедура отримання якого значно складніша та довша, потрібно встановлювати спеціальний плагін або завжди мати в доступі флешку, а також зберігати ключі лише на флешці або робочому комп'ютері [7].

SmartID після створення можна використовувати для формування звітів, укладання та підписування договорів, платежів та доступу до ресурсів і сервісів, таких як Дія,

ID.GOV.UA. тощо. Це означає, що складний процес для отримання кваліфікованого електронного підпису, має альтернативу, його отримати значно простіше, кожна особа має доступ до процедури SmartID з будь якої точки України та навіть поза її межами. Крім цього ризик знищення фізичного носія КЕП буде відсутнім, що зараз, під час бойових дій, є надзвичайно актуальним.

Для регулювання послуг, схожих на SmartID, був запроваджений Закон України «Про хмарні послуги», метою якого було створення умов для здійснення хмарних послуг, у тому числі державними органами з надавачами таких послуг, як на території країни, так і поза її межами. На практиці, що важливо в умовах воєнного стану, органи державної влади дали дозвіл на розміщення публічних реєстрів, інформаційних даних та їх копій на хмарних ресурсах чи в центрах обробки даних, які розташовані за межами України [8].

Наприклад, Національний банк України постановою № 42 від 8 березня 2022 року, надав доручення іншим банківським установам використовувати хмарні ресурси, що розташовані за кордоном, з метою забезпечення належної обробки персональних даних клієнтів.

Варто зазначити, що з метою захисту персональних даних працівників, що мають доступ до персональних даних, виконують письмове зобов'язання щодо нерозголошення персональних даних, які їм були відомі чи довірені у зв'язку з виконанням професійних чи службових або трудових обов'язків. Суб'єкти, які обробляють дані, на усіх рівнях мають забезпечити захист останніх шляхом вжиття спеціальних технічних заходів захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних [9].

Постає питання про реалізацію вказаних положень на практиці, оскільки через постійну небезпеку, нестабільний Інтернет та відсутність електромережі не завжди є змога здійснювати належну обробку даних. Відтак, є потреба у розгляді даної проблеми з метою недопущення порушення встановленого законодавством права особи щодо захисту її персональних даних та забезпечення безпечного укладання договорів.

Наприклад, із цією метою було внесено зміни до Кримінального процесуального кодексу України щодо проведення слідчих дій. Прокурор, відповідно до нових правил, передбачених ст. 615 КПК України та Прикінцевими положеннями останнього, може санкціонувати тимчасовий доступ до таких джерел, як лікарська, банківська таємниця, персональні дані, що знаходяться у особистому володінні чи в базі персональних даних цієї особи, даних операторів та провайдерів комунікацій при погодженні з керівником прокуратури [10; 11].

Однак широкий перелік доступу до даних особи спричиняє недосконалість таких змін, оскільки не є зрозумілим, в чому виявляється цінність та необхідність розкриття саме цих відомостей особи, та яке значення останніх під час воєнного стану. Доцільним є внесення змін до законодавства з метою деталізації приватних даних, до яких є необхідним доступ державних органів в умовах воєнного стану, та створення окремого законодавчого нормативно-правового акту, який міститиме перелік випадків, щодо яких може застосовуватися такий тимчасовий доступ органів прокуратури тощо.

Щодо сутності Mobile ID – це технологія дистанційної ідентифікації, автентифікації електронного цифрового підпису (ЕЦП) фізичних осіб у інформаційно-телекомунікаційних системах. Вона передбачає зберігання особистих ключів електронного підпису на SIM-карті та передачу даних через SMS. Експерти у цій сфері бачать за цією технологією майбутнє і широкі можливості, адже вона здатна забезпечити одночасно простоту, безпеку та мак-

симальну мобільність користувача у процесі отримання електронних послуг [12].

В Україні вже сформувався попит на взаємодію в електронній формі серед учасників цивільного обороту. Представники комерційної сфери, розуміючи які конкурентні переваги несе цифрова трансформація, готові в електронному вигляді оформляти договори та здійснювати транзакції. У вартість транзакційних витрат включаються різноманітні послуги юристів, нотаріусів, бухгалтерів, а також банківські комісії. Зокрема, при оформленні договору купівлі-продажу нерухомості (ст. 655 ЦК України) необхідно оплатити послуги нотаріусів, оцінювачів, банківських установ тощо [1].

Наші співвітчизники дедалі активніше використовують портали державних послуг – підписують петиції на сайті офіційного інтернет-представництва Президента України, органів місцевого самоврядування, замовляють виписки і довідки, отримують субсидії на сайті Міністерства соціальної політики України, реєструють бізнес тощо. Наприклад, при укладанні декларації з сімейним лікарем її можна «підписати» кодом з SMS, онлайн можна замовити комп'ютер (ст. 712 ЦК України) чи оформити мікrokредит. У кожному з цих випадків укладається договір з електронним підписом.

Розробники та користувачі зазначених електронних послуг схильні вважати, що найбільшими перевагами нововведень є безпека, приватність, доступність і зручність технології Mobile ID, яка дозволить значно розширити аудиторію електронних послуг і забезпечити безпеку відповідних транзакцій.

Проте на шляху розвитку електронного урядування та електронної комерції виникає серйозний бар'єр – відсутність надійних, доступних і безпечних засобів електронної ідентифікації громадян. Зважаючи, що на сьогодні практично весь вітчизняний ринок стільникового зв'язку перебуває під контролем сторонніх суб'єктів господарювання, потребує першочергово врегулювання питання захисту інформації вітчизняними операторами стільникового зв'язку при наданні послуги Mobile ID.

Доступ до електронних довірчих послуг може отримуватись споживачами зі стаціонарних комп'ютерів або мобільних телекомунікаційних пристроїв (смартфонів, планшетів тощо). Однією з нагальних проблем користування електронними довірчими послугами з мобільного пристрою вбачається вибір оптимальної технології формування у ньому кваліфікованого електронного цифрового підпису. У стільниковому зв'язку на зазначеній технології засновується мобільний сервіс Mobile ID, який на вітчизняному ринку телекомунікацій запроваджено мобільними операторами «Київстар», «Водафон» і «Лайфселл» [13].

При наданні електронних довірчих послуг особа ідентифікується за ЕЦП, який генерується криптографічними методами і засобами. При цьому електронні дані, паперові аналоги яких мають містити власноручний підпис особи, надаються з використанням її кваліфікованого електронного підпису. Останній повинен формуватись засобами, які мають документ чи позитивний експертний висновок державної експертизи у сфері криптографічного захисту інформації щодо відповідності вимогам, які встановлюються Кабінетом Міністрів України, що передбачено, зокрема, ч. 2 ст. 17, ч. 3 ст. 19 Закону України «Про електронні довірчі послуги» [3].

Для користування Mobile ID абонент отримує у центрі обслуговування абонентів оператора мобільного зв'язку спеціальну Sim-картку з модулем зберігання першої половини криптографічного ключа ЕЦП і програмних засобів його створення (криптомодуля). У цілях безпеки ЕЦП, програмні засоби його формування не повинні зчитуватись жодними іншими програмними засобами.

Доречно зазначити, що з урахуванням умов воєнного стану, зріс попит на укладання, розірвання чи при-

пинення договорів саме у електронній формі. Зокрема, внаслідок переміщення громадян України країною та за кордон, у багатьох немає змоги розірвати раніше укладений договір оренди житла (ст. 810 ЦК України). Проте відтепер, угоду про розірвання договору найму житла можна підписати у електронній формі з використанням КЕП, Mobile-ID, а крім цього, аналогічні дії можна вчинити щодо укладання договору оренди житлового приміщення. Схоже передбачено ст. ст. 909, 1029, 1031, 1046, 1131 ЦК України.

Висновок. Запровадження інструментів електронної ідентифікації з використанням кваліфікованого електронного підпису, мобільного цифрового підпису має перспективне значення у подальшому розвитку та запровадженні

аналогічних систем, однак потребує законодавчого вдосконалення з метою захисту приватності особи. Можливість використання цих систем для укладання цивільно-правових договорів в умовах збройного конфлікту РФ проти України дозволило здійснити якісний та кількісний перехід до цифрового та інформаційного суспільства з широким використанням інформаційно-комунікаційних технологій при здійсненні юридично значущих дій, автоматизації документообігу, забезпечення їх прозорості і законності. Проблематикою для подальших наукових досліджень є окремі аспекти гарантування безпеки укладання таких правочинів в умовах воєнного стану з метою здійснення належного захисту прав та інтересів учасників цивільного обороту.

ЛІТЕРАТУРА

1. Цивільний кодекс України : Кодекс України від 16.01.2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 23.12.2022).
2. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text> (дата звернення: 23.12.2022).
3. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> (дата звернення: 23.12.2022).
4. Конституція України від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254k/96-вр#Text> (дата звернення: 23.12.2022).
5. Алла Король. Термін дії ЕЦП подовжено на час воєнного стану – рішення Кабміну. *БУХГАЛТЕР.UA* : вебсайт. URL: https://buh.ligazakon.net/news/210036_termn-d-etsp-podovzheno-na-chas-vonnogo-stanu-rshennya-kabmnu (дата звернення: 23.12.2022).
6. Удосконалений Е-підпис: ДПС роз'яснила особливості його використання : Офіційне видання державної фіскальної служби України. URL: <http://www.visnuk.com.ua/uk/news/100025797-udoskonaleniy-e-pidpis-dps-roz-yasnila-osoblivosti-yogo-vikoristannya> (дата звернення: 23.12.2022).
7. Кваліфікований електронний підпис SmartID. *Приватбанк* : вебсайт. URL: <https://privatbank.ua/smart-id> (дата звернення: 23.12.2022).
8. Про хмарні послуги : Закон України від 17.02.2022 р. № 2075-IX. URL: <https://zakon.rada.gov.ua/laws/show/2075-20#Text> (дата звернення: 23.12.2022).
9. Рекомендації щодо захисту персональних даних в умовах воєнного стану. *Уповноважений Верховної Ради України з прав людини* : вебсайт. URL: https://ombudsman.gov.ua/news_details/rekomendaciyi-shchodo-zahistu-personalnih-danih-v-umovah-voyennogo-stanu (дата звернення: 23.12.2022).
10. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про попереднє ув'язнення» щодо додаткового регулювання забезпечення діяльності правоохоронних органів в умовах воєнного стану : Закон України від 03.03.2022 р. № 2111-IX. URL: <https://zakon.rada.gov.ua/laws/show/2111-20#Text> (дата звернення: 23.12.2022).
11. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 р. № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 23.12.2022).
12. Для чого потрібен Mobile ID та як ним користуватися? Я маю право! URL: <https://pravo.minjust.gov.ua/ua/explanation/1495-dlyachogo-potriben-mobile-id-ta-jak-nim-koristuvatisya> (дата звернення: 23.12.2022).
13. Чеславський О. Mobil-ID та Smart-ID – в чому різниця? *Київлада* : вебсайт. URL: <https://kievlast.com.ua/mind/mobil-id-ta-smart-idv-chomu-riznitsya-perevag-i-nedoliki> (дата звернення: 23.12.2022).