УДК 342.951

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ПРОВАЙДЕРА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ЯК СУБ'ЄКТА ПРАВОВІДНОСИН У СФЕРІ ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ

Стаття присвячена державному регулюванню діяльності провайдерів електронних довірчих послуг, класифікації провайдерів електронних довірчих послуг, дослідженню їх прав, обов'язків та відповідальності. Автором приділено увагу відмінностям правового статусу кваліфікованих та некваліфікованих провайдерів, перевагам користування послугами кваліфікованих провайдерів електронних довірчих послуг. Проведено порівняльний аналіз правового статусу провайдера довірчих послуг за законодавством України та правом Європейського Союзу.

Ключові слова: електронні довірчі послуги, провайдер електронних довірчих послуг, електронна ідентифікація, електронний підпис.

Білоцерковець Назар Вікторович,
аспірант кафедри адміністративного права юридичного факультету Київського національного університету імені Тараса Шевченка
nazar.oazis@gmail.com

1. Вступ

Ефективне державне регулювання правовідносин у сфері надання й отримання електронних довірчих послуг є важливою передумовою для впровадження в Україні електронного урядування, а також новітнього механізму електронної комерції. Наявність у процесах передання інформації багаторівневих взаємин учасників зумовлює необхідність виділення низки самостійних суб'єктів із конкретизованими повноваженнями. Тому аналіз правового статусу такого суб'єкта, як провайдер електронних довірчих послуг, є безумовно важливим для розвитку електронного урядування в Україні.

Предметом уваги вітчизняних і зарубіжних дослідників були переважно питання, пов'язані з визначенням правового статусу суб'єктів надання й використання окремих видів електронних довірчих послуг, зокрема електронного цифрового підпису. Серед науковців, які займалися вивченням цих питань, варто назвати В.І. Квашніна, Р.О. Халікова, П.С. Симоновича, Д.В. Шибаєва та інших. Водночас поза увагою цих дослідників залишилися проблемні аспекти, пов'язані з формуванням інституту електронних довірчих послуг загалом та їх державного регулювання зокрема. Тому дослідження особливостей державного регулювання діяльності провайдерів електронних довірчих послуг крізь призму їхніх прав, обов'язків та відповідальності є надзвичайно актуальним.

Важливість розгляду цього питання зумовлюється також прийняттям Закону України «Про електронні довірчі послуги» (далі – Закон), який набирає чинності 7 листопада 2018 р. Адміністративно-правовим відносинам у цій сфері присвячені ст. ст. 5–10, 17 та 30 Закону, які регулюють також порядок набуття статусу кваліфікованого провайдера електронних довірчих послуг, встановлення до них вимог із безпеки й захисту інформації, захисту персональних даних, проведення процедур оцінки відповідності кваліфікованих провайдерів, накладення на них адміністративних штрафів та вимоги щодо припинення їх діяльності. Закон також встановлює особливі вимоги до електронної взаємодії громадян із суб'єктами публічної адміністрації за посередництва провайдерів електронних довірчих послуг.

Тому метою статті є дослідження державного регулювання діяльності суб'єктів, які надають не лише послуги електронного цифрового підпису, а й інші електронні довірчі послуги, що передбачені або мають бути передбачені законом.

2. Класифікація суб'єктів правовідносин у сфері електронної ідентифікації та електронних довірчих послуг

У науці існують різні підходи до класифікації та найменувань суб'єктів правовідносин у сфері електронної ідентифікації та електронних довірчих послуг.

Ми пропонуємо класифікувати суб'єктів правовідносин у сфері електронної ідентифікації та електронних довірчих послуг залежно від їх правового статусу на такі три групи: *1) провайдери електронних довірчих послуг (посередники)*; 2) користувачі довірчих послуг (безпосередні учасники документообігу); 3) суб'єкти державного регулювання у сфері електронної ідентифікації. Така класифікація є технологічно нейтральною, адже може бути застосована не лише до «криптографічних» засобів ідентифікації, а й до засобів, що ґрунтуються на будь-яких інших технологіях. Крім цього, вона може бути застосована не тільки до електронних підписів, а й до інших електронних довірчих послуг.

3. Класифікація провайдерів електронних довірчих послуг

Залежно від дотримання провайдером спеціальних вимог до рівня безпеки послуг, що встановлюються державою, Регламентом (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 р. про електронну ідентифікацію та довірчі послуги для електронних транзакцій у межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС (далі – Регламент) провайдери поділяються на кваліфікованих і некваліфікованих.

Регламент встановлює суттєву різницю між кваліфікованим провайдером, кваліфікованою довірчою послугою, з одного боку, та некваліфікованим провайдером, некваліфікованою довірчою послугою – з іншого.

Залежно від виду послуг, що надаються, пропонуємо класифікувати провайдерів електронних довірчих послуг на суб'єктів надання послуг електронної сертифікації, електронної печатки, датування, електронних відправлень, автентифікації веб-сайтів, електронного архівування тощо.

У межах цієї групи провайдери також можуть бути розділені на декілька підгруп. Так, Д. Мутон зазначає, що до провайдерів послуг електронної сертифікації належать такі: 1) власне суб'єкт сертифікації; 2) суб'єкт реєстрації (установа, яка встановлює особу-заявника на отримання сертифіката електронного підпису);

3) оператор сертифікації (установа, яка забезпечує роботу технічної інфраструктури з видачі сертифікатів); 4) суб'єкт верифікації (установа, яка здійснює перевірку чинності сертифікатів); 5) суб'єкт анулювання (установа, яка вносить сертифікат до списку відкликаних сертифікатів) (Mouton, 2011). Е.А. Капріолі додає до цього переліку суб'єкта публікування (установа, яка забезпечує ведення списку відкликаних сертифікатів) (Caprioli, 2014).

Залежно від кола суб'єктів, яким провайдери надають послуги, їх класифікують на провайдерів систем загального користування та провайдерів корпоративних систем (Халиков, 2006).

4. Загальні обов'язки провайдерів електронних довірчих послуг

З огляду на запропоновану класифікацію провайдерів електронних довірчих послуг обов'язки останніх доцільно поділити на загальні (стосуються всіх провайдерів електронних довірчих послуг) і спеціальні (стосуються виключно кваліфікованих провайдерів).

Французький науковець Е. Жакмен *до обов'язків усіх провайдерів* відносить обов'язки з дотримання вимог щодо безпеки, обов'язки у сфері обробки персональних даних, обов'язки у сфері забезпечення доступності послуг для осіб з обмеженими можливостями (Jacquemin, 2016).

Статтею 8 Закону передбачено, що до повноважень Адміністрації Державної служби спеціального зв'язку та захисту інформації України належить встановлення вимог до провайдерів електронних довірчих послуг із безпеки й захисту інформації. Водночас серед принципів державного регулювання вказаної сфери Закон визначає відповідність вимог до надання електронних довірчих послуг європейським і міжнародним стандартам.

У зв'язку із цим пропонуємо дослідити європейські та міжнародні стандарти державного регулювання діяльності провайдерів електронних довірчих послуг.

Так, з метою дотримання вимог у сфері безпеки провайдери довірчих послуг повинні вжити відповідні технічні та організаційні заходи з управління ризиками, що пов'язані з безпекою довірчих послуг, які вони надають (ст. 19 Регламенту). Беручи до уваги останні технічні досягнення, рівень гарантії повинен пропорційно відповідати ступеню ризику. Зокрема, мають вживатися заходи для запобігання та мінімізації наслідків інцидентів у галузі безпеки, а також інформування зацікавлених сторін про їх негативні наслідки. Крім цього, згідно із ч. 2 ст. 19 Регламенту на провайдерах довірчих послуг лежить обов'язок повідомити орган контролю, інші компетентні органи, користувачів про порушення безпеки чи втрату цілісності протягом 24 годин після того, як їм стало відомо про це.

Проблемою законодавчого регулювання правового статусу провайдерів довірчих послуг (центрів сертифікації) в Україні є відсутність законодавчого обов'язку центру сертифікації повідомляти уповноважені органи виконавчої влади про факти стороннього втручання в його діяльність.

У світовій практиці мають місце випадки зловживання центрами сертифікації своїм правовим статусом у зв'язку з відсутністю такого обов'язку. Так, данський центр сертифікації «DigiNotar» у 2011 р. став об'єктом хакерської атаки, у результаті якої була викрадена значна кількість закритих ключів. Злочинці спромоглися «видати»

фальшивий сертифікат, який у подальшому був наданий одному з веб-сайтів компанії «Google» та використаний для незаконного стеження за громадянами Ірану. Посадовим особам «DigiNotar» було відомо про таке втручання, однак вони замовчували про нього з метою збереження репутації, що в результаті призвело до завдання значної майнової шкоди учасникам електронного документообігу (Massacci, Gadyatskaya, 2011).

У зв'язку із цим ми підтримуємо закріплення такого обов'язку провайдерів електронних довірчих послуг у ч. 2 ст. 12 Закону, який набирає чинності 7 листопада 2018 р.

До загальних обов'язків провайдерів електронних довірчих послуг також відносять такі:

– гарантувати унікальність сертифіката ключа підпису;

– вести реєстр сертифікатів ключів підпису та надавати учасникам можливість доступу до нього;

– забезпечувати доступність відкритого ключа для всіх заінтересованих осіб;

– зберігати видані сертифікати в електронному вигляді після закінчення строку дії сертифікатів ключів протягом визначеного часу;

– забезпечувати актуальність ключів;

– своєчасно вносити дані про призупинені чи анульовані ключі (Шибаев, 2011);

– призупиняти дію сертифіката в передбачених законом випадках;

– повідомляти власника сертифіката про факти, які суттєвим чином можуть позначитись на можливості подальшого використання сертифіката (Квашнин, 2010);

– зберігати інформацію, внесену до реєстру сертифікатів ключів (Суворов, 2010).

5. Обов'язки кваліфікованих провайдерів довірчих послуг

Якщо відносини між користувачами та «звичайними» провайдерами довірчих послуг мають переважно приватноправовий характер, а обов'язки останніх визначаються зазвичай у договорі, то права й обов'язки кваліфікованих провайдерів є предметом державного регулювання. Зазначену тезу недвозначно підтверджує зміст ст. 13 Закону.

З метою адаптації державного регулювання цієї сфери до міжнародних стандартів варто проаналізувати підходи зарубіжних науковців та європейського законодавця до вирішення цього питання.

Обов'язки кваліфікованих провайдерів передбачені, зокрема, у ч. 2 ст. 24 Регламенту, яка перелічує обов'язки щодо інформування наглядового органу: інформування користувачів (п. «a»), професіоналізму персоналу та субпідрядників (п. «b»), фінансових ресурсів та страхування (п. «c»), надійності та безпеки систем і продуктів (п. п. «d»–«g»), зберігання інформації (п. «h»), продовження та припинення діяльності (п. «i»). Наприклад, провайдер, який надає одночасно кваліфіковані та некваліфіковані послуги, не може інформувати користувачів про надання ним лише кваліфікованих послуг, адже користувачі, отримуючи некваліфіковану послугу, вважатимуть, що отримують кваліфіковану (Gobert, 2016).

Особливу увагу європейський законодавець приділяє державному регулюванню процедури припинення діяльності кваліфікованих провайдерів.

Регламент зобов'язує провайдерів мати власні плани припинення діяльності та зберігати дані, видані або отримані провайдером, з метою забезпечення безперервності надання послуг (ст. ст. 17 та 24 Регламенту).

Національне законодавство країн Європейського Союзу передбачає обов'язок кваліфікованого провайдера (у разі припинення діяльності за власним бажанням) передати свою діяльність іншому кваліфікованому провайдеру як правонаступнику; якщо це неможливо, він повинен вжити всіх заходів, щоб максимально зменшити шкоду, яка може бути завдана користувачам. Про свій намір припинити діяльність він має повідомити орган контролю, який здійснюватиме нагляд за дотриманням провайдером вимог законодавства під час процедури припинення діяльності (Gobert, 2016).

Натомість Закон не передбачає можливість передання сертифікатів ключів припиненого провайдера на обслуговування до іншого провайдера.

Вважаємо, що для забезпечення безперервності й довгостроковості електронних довірчих послуг, а також задля збільшення рівня довіри користувачів цих послуг держава повинна чітко врегульовувати порядок припинення діяльності провайдерів та унеможливлювати будь-які ризики для користувачів довірчих послуг у таких випадках.

Регламент також зобов'язує кваліфікованих провайдерів проходити аудит із боку органу з оцінки відповідності. Він має здійснюватися кожні 24 місяці за рахунок провайдера. Цей аудит, згідно із ч. 2 ст. 20 Регламенту, може бути здійснений у будь-який час за запитом контролюючого органу.

З викладеного постає, що в європейському законодавстві, а також у науковій літературі висуваються жорсткі вимоги до діяльності кваліфікованих провайдерів електронних довірчих послуг.

Водночас високий рівень вимог до кваліфікованих провайдерів електронних довірчих послуг має наслідком отримання користувачами їхніх послуг низки переваг, зокрема: а) презумпція застосування принципу асиміляції; б) презумпція дотримання всіх необхідних вимог та виконання всіх обов'язкових функцій; в) міжнародне визнання; г) збільшені розміри санкцій. З іншого боку, некваліфіковані довірчі послуги не користуються жодними презумпціями, а їх доказова сила підлягає доведенню в суді.

На нашу думку, можливість застосування цих презумпцій зумовила включення до Закону норми, за якою електронна взаємодія фізичних і юридичних осіб із суб'єктами владних повноважень повинна здійснюватися з використанням лише тих електронних довірчих послуг, які надаються кваліфікованими провайдерами (ч. 2 ст. 17 Закону).

У зв'язку із цим пропонуємо з'ясувати, чому кваліфіковані електронні довірчі послуги є більш надійним та зручним засобом офіційної комунікації із суб'єктами владних повноважень, ніж некваліфіковані довірчі послуги.

Що стосується *презумпції застосування принципу асиміляції,* то відповідно до ч. 2 ст. 25 Регламенту юридична сила електронного кваліфікованого підпису є еквівалентною юридичній силі власноручного підпису. Застосування цієї презумпції щодо інших довірчих послуг врегульоване в ч. 2 ст. 43 Регламенту (презумпція

цілісності даних, відправлених кваліфікованим електронним листом, презумпція передачі даних ідентифікованим відправником та отримання ідентифікованим отримувачем), у ч. 2 ст. 41 Регламенту (презумпція точності дати й часу, на які вказує кваліфікована електронна позначка часу, і цілісності даних, з якими ці дата та час пов'язані), у ч. 2 ст. 35 Регламенту (презумпція цілісності й точності походження даних, скріплених кваліфікованою печаткою). Для електронної автентифікації веб-сайту жодної презумпції не передбачено.

Такі презумпції Д. Гобер називає спростовними, адже презумпції цілісності даних, точності дати й часу тощо можуть бути спростовані в суді особою, яка їх оскаржує (Gobert, 2016). Тому, на нашу думку, закон має передбачати можливість їх спростування іншою стороною.

Презумпція дотримання всіх необхідних вимог та виконання всіх обов'язкових функцій означає, що в разі, якщо законодавство прямо чи опосередковано зобов'язує використовувати рекомендоване електронне відправлення, проставляти на документі дату й час його вчинення, зберігати копії документів, то цей обов'язок вважається належним чином виконаним, якщо було використано послугу кваліфікованого рекомендованого електронного відправлення, кваліфікованої позначки часу, кваліфіковану послугу електронного архівування відповідно.

Цю презумпцію Д. Гобер називає неспростовною (Gobert, 2016).

На нашу думку, не випадково у вказаному вченим переліку відсутня довірча послуга електронного підпису. Адже обов'язок використовувати кваліфіковані електронні підписи в усіх випадках, коли законодавство вимагає підписання документа, суперечило б меті Регламенту спростити відносини електронного документообігу та взагалі унеможливило б використання простих і некваліфікованих удосконалених підписів.

Для належного функціонування внутрішнього ринку Європейського Союзу Регламент передбачає *взаємне визнання* кваліфікованих електронних довірчих послуг однієї держави-члена в інших державах членах (для електронних підписів – ч. 3 ст. 25 Регламенту, для електронних печаток – ч. 3 ст. 35 Регламенту, для електронних позначок часу – ч. 3 ст. 41 Регламенту).

Дивним, на наше переконання, видається те, що стосовно кваліфікованих рекомендованих електронних відправлень та автентифікації веб-сайтів жодних положень про взаємне визнання Регламент не передбачає.

Що стосується *збільшених розмірів санкцій* кваліфікованих провайдерів, то відповідно до ч. 1 ст. 13 Регламенту всі провайдери довірчих послуг повинні нести відповідальність за збиток, заподіяний навмисно або з недбалості будь-якій фізичній чи юридичній особі в результаті недотримання зобов'язань, передбачених Регламентом. При цьому Регламент презюмує, що кваліфікований провайдер діяв умисно або з необережності, тоді як у випадку з некваліфікованими надавачами потерпіла особа має довести ці обставини.

Водночас такий підхід критикується європейськими науковцями, які стверджують, що центр сертифікації лише вносить до сертифіката інформацію про майбутнього його власника, що міститься в офіційних документах, які надаються центру сертифікації. Однак у разі фальсифікації, як матеріальної (підробки матеріальних

носіїв), так і інтелектуальної (надання недостовірної інформації), провайдер не повинен нести відповідальність за інформацію, що була розміщена ним у сертифікаті. Також пропонується виключити можливість настання відповідальності центру сертифікації в разі, якщо користувач не перевірив факт припинення дії сертифіката у відповідному реєстрі, а також у разі використання сертифіката з порушенням меж його використання, вказаних у самому сертифікаті (Caprioli, 2014).

У цьому контексті пропонуємо імплементувати в законодавство України підхід французького законодавця, який передбачає, що доказом того, що центр сертифікації діяв обережно, може бути висновок незалежного аудитора, складений за результатами перевірки цього центру (Caprioli, 2014).

6. Права провайдерів електронних довірчих послуг

До прав, які належать усім провайдерам довірчих послуг, варто віднести такі:

– надавати електронні довірчі послуги в порядку, передбаченому законом (у тому числі виготовляти сертифікати ключів підписів, створювати ключі для учасників електронного документообігу) (Шибаев, 2011);

– делегувати частину своїх повноважень стороннім організаціям, наприклад, делегувати повноваження щодо прийняття заявок на виготовлення сертифікатів ключів підписів (така практика існує в європейських країнах (Caprioli, 2014), однак критикується російськими науковцями, які переконані, що таке делегування ставить під загрозу встановлення автентичності електронного підпису (Квашнин, 2010)).

Як європейський, так і вітчизняний законодавці закріплюють за кваліфікованими провайдерами право бути включеним до довірчого списку.

На відміну звичайного провайдера кваліфікований провайдер довірчих послуг може почати надавати кваліфіковану послугу після того, як інформацію про статус буде внесено до довірчих списків (ст. 21 Регламенту та ст. 30 Закону). Із цього моменту вони можуть використовувати знак довіри Європейського Союзу для кваліфікованих довірчих послуг. З іншого боку, довірчий список, ведення якого буде покладене на Міністерство юстиції України, є також засобом, який робить контроль із боку держави за діяльністю кваліфікованих провайдерів більш ефективним.

7. Відповідальність провайдерів електронних довірчих послуг

У науковій літературі пропонуються певні підстави класифікації підстав відповідальності провайдерів електронних довірчих послуг. Так, П.С. Симонович пропонує розрізняти відповідальність засвідчувальних центрів за якість послуг, що надаються, і відповідальність за зберігання та/або передання інформації протиправного характеру (Симонович, 2004).

У європейській літературі залежно від суб'єктів і механізму покладення на них відповідальності виділяють відповідальність центрів, що надають послуги електронної сертифікації, відповідальність центрів, що надають послуги шифрування (криптології), та відповідальність центрів, що надають довірчі послуги загалом (Caprioli, 2014).

На нашу думку, з огляду на описані вище відмінності в правовому статусі кваліфікованих та некваліфікованих провайдерів довірчих послуг необхідно також окремо виділяти механізм покладення відповідальності на кваліфікованих і некваліфікованих провайдерів.

Досліджуючи питання відповідальності провайдерів електронних довірчих послуг, варто приділити увагу страхуванню відповідальності цих суб'єктів. Ми згодні з доводами науковців про необхідність страхування відповідальності провайдерів довірчих послуг (Caprioli, 2014).

Низка науковців стверджують про необхідність встановлення на законодавчому рівні вимог до матеріальних і фінансових можливостей акредитованих засвідчувальних центрів (кваліфікованих провайдерів – Н. Б.) з метою відшкодування ними шкоди, заподіяної третім особам (Суворов, 2010; Шибаев, 2011; Халиков, 2006), а також встановлення меж їх відповідальності (Квашнин, 2010).

Водночас провайдери довірчих послуг можуть нести також адміністративну відповідальність. Цікавим у цьому плані є досвід Бельгії, законодавство якої дозволяє ув'язнення на строк до 1 року або штраф у розмірі до 100 000 євро на провайдера, який позиціонує себе як кваліфікований, проте не є таким (Didier, 2016).

8. Висновки

За результатами дослідження пропонуємо визначити провайдера електронних довірчих послуг як юридичну особу будь-якої організаційно-правової форми чи фізичну особу – підприємця, які надають кваліфіковані та/або некваліфіковані електронні довірчі послуги користувачам таких послуг на платній чи безоплатній основі, мають права й обов'язки та несуть юридичну відповідальність, визначені законом і договором із користувачем. При цьому кваліфікованим провайдером електронних довірчих послуг є провайдер електронних довірчих послуг, який виконує спеціальні вимоги щодо діяльності у сфері надання електронних довірчих послуг та відомості про якого внесені до спеціального довірчого списку, унаслідок чого він може надавати кваліфіковані довірчі послуги. Саме кваліфіковані довірчі послуги можуть використовуватися для електронної взаємодії фізичних і юридичних осіб із публічною адміністрацією. Тому державне регулювання у сфері електронних довірчих послуг значною мірою спрямоване на встановлення прав та обов'язків кваліфікованих провайдерів, відповідності їх діяльності вимогам міжнародних стандартів, підстав і порядку притягнення їх до адміністративної відповідальності.

Список використаних джерел:

1. Шибаев Д.В. Унификация организационно-правового обеспечения электронного документооборота органов государственной власти субъектов Российской Федерации: дисс. … канд. юрид. наук: 12.00.14. Москва, 2011. 249 с.

2. Об электронном документе: проект Федерального закона Российской Федерации от 20 декабря 2000 г. № КВЯ/82 / Государственная Дума. URL: http://www.libertarium.ru/25162.

3. Шамраев А.В. Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. Москва: Статут; Интертех; БДЦ-пресс, 2003. 1013 с.

4. Квашнин В.И. Правовые аспекты использования электронной цифровой подписи в договорных отношениях с участием предпринимателей: дисс. … канд. юрид. наук: 12.00.03. Санкт-Петербург, 2010. 225 с.

5. Colin J.-N. Du secret a la confiance… quelque elements de cryptographie. Jacquemin H. L'identification electronique et les services de confiance depuis le Reglement eIDAS. Bruxelles: Edition Larcier, 2016. P. 7–28.

6. Mouton D. Securite de la dematerialization. Paris: Groupe Eyrolles, 2012. 314 p.

7. Caprioli E.A. Signature electronique et dematerialization. Paris: LexisNexis SA, 2014. 400 p.

8. Халиков Р.О. Правовой режим электронного документа: вопросы использования электронной цифровой подписи: дисс. … канд. юрид. наук: 12.00.03. Казань, 2006. 189 с.

9. Jacquemin H. Principes applicables a tous les services de confiance et au document electronique. Jacquemin H. L'identification electronique et les services de confiance depuis le Reglement eIDAS. Bruxelles: Edition Larcier, 2016. P. 101–138.

10. Massacci F., Gadyatskaya O. How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results. Universita degli studi di Trento. White paper. 2013. URL: http://www.cspforum.eu/Seccord_eidas_whitepaper_2013.pdf.

11. Суворов А.А. Административно-правовые основы деятельности удостоверяющих центров электронной цифровой подписи в Российской Федерации: автореф. дисс. … канд. юрид. наук: 12.00.14 «Административное право; финансовое право; информационное право». Москва, 2010. 26 с.

12. Didier G. La loi belge de 21 Juillet 2016 mettant en oeuvre le reglement europeen eIDAS et le completant avec des regles sur l'archivage electronique: analyse approphondie. URL: https://www.droit-technologie.org/wp-content/uploads/2016/11/annexes/dossier/276-1.pdf.

13. Симонович П.С. Правовое регулирование отношений, связанных с совершением сделок в электронных информационных сетях в России, США и ЕС: автореф. дисс. … канд. юрид. наук: 12.00.03 «Гражданское право; предпринимательское право; семейное право; гражданский процесс; международное частное право». Москва, 2004. 24 с.

References:

1. Shibaev, D.V. (2011). Unifikatsiia organizatsionno-pravovogo obespecheniia elektronnogo dokumentooborota organov gosudarstvennoi vlasti subieektov Rossiiskoi Federatsii [Unification of organizational and legal support for electronic document circulation of state authorities of the subjects of the Russian Federation] (PhD Thesis). Moscow. [in Russian].

2. The State Duma (2000). Ob elektronnom dokumente: proekt Federalnogo zakona Rossiiskoi Federatsii [On the electronic document: the draft Federal Law of the Russian Federation]. Retrieved from: http://www.libertarium.ru/25162.

3. Shamraev, A.V. (2003). Pravovoe regulirovanie informatsionnykh tekhnologii (analiz problem i osnovnye dokumenty). Versiia 1.0 [Legal regulation of information technologies (analysis of problems and basic documents). Version 1.0]. Moscow: Statut; Intertekh; BDTS-press. [in Russian].

4. Kvashnin, V.I. (2010). Pravovye aspekty ispolzovaniia elektronnoi tsifrovoi podpisi v dogovornykh otnosheniiakh s uchastiem predprinimatelei [Legal aspects of the use of electronic digital signature in contractual relations with the participation of entrepreneurs] (PhD Thesis). Sankt-Peterburg. [in Russian].

5. Colin, J.-N. (2016). Du secret a la confiance… quelque elements de cryptographie. L'identification electronique et les services de confiance depuis le Reglement eIDAS. Bruxelles: Edition Larcier, pp. 7–28.

6. Mouton, D. (2012). Securite de la dematerialization. Paris: Groupe Eyrolles. [in French].

7. Caprioli, E.A. (2014). Signature electronique et dematerialization. Paris: LexisNexis SA. [in French].

8. Khalikov, R.O. (2006). Pravovoi rezhim elektronnogo dokumenta: voprosy ispolzovaniia elektronnoi tsifrovoi podpisi [Legal regime of the electronic document: issues of using an electronic digital signature] (PhD Thesis). Kazan. [in Russian].

9. Jacquemin, H. (2016). Principes applicables a tous les services de confiance et au document electronique. L'identification electronique et les services de confiance depuis le Reglement eIDAS. Bruxelles: Edition Larcier, pp. 101–138.

10. Massacci, F., Gadyatskaya, O. (2013). How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results. Universita degli studi di Trento. White paper. Retrieved from: http://www.cspforum.eu/Seccord_eidas_whitepaper_2013.pdf.

11. Suvorov, A.A. (2010). Administrativno-pravovye osnovy deiatelnosti udostoveriaiushchikh tsentrov elektronnoi tsifrovoi podpisi v Rossiiskoi Federatsii [Administrative and legal basis for the activities of the certification centers for electronic digital signatures in the Russian Federation] (author's abstract of the dissertation of the candidate of juridical science). Moscow. [in Russian].

12. Didier, G. (2016). La loi belge de 21 Juillet 2016 mettant en oeuvre le reglement europeen eIDAS et le completant avec des regles sur l'archivage electronique: analyse approphondie. Retrieved from: https://www.droit-technologie.org/wp-content/uploads/2016/11/annexes/dossier/276-1.pdf.

13. Simonovich, P.S. (2004). Pravovoe regulirovanie otnoshenii, sviazannykh s soversheniem sdelok v elektronnykh informatsionnykh setiakh v Rossii, SSHA, i ES [Legal regulation of relations related to transactions in electronic information networks in Russia, the United States and the EU] (author's abstract of the dissertation of the candidate of juridical science). Moscow. [in Russian].

STATE REGULATION OF ACTIVITIES OF ELECTRONIC TRUST SERVICES PROVIDER OF AS A PARTY TO LEGAL RELATIONS IN THE FIELD OF ELECTRONIC IDENTIFICATION

Nazar Bilotserkovets,
Postgraduate Student at the Department of Administrative Law of Faculty of Law of Taras Shevchenko National University of Kyiv
nazar.oazis@gmail.com

The purpose of this article is to determine the legal status of entities that provide not only digital signature services but also other electronic trust services by examining their rights, obligations and legal responsibility. Special attention is paid to state regulation of their activities as well as their administrative liability.

This article is based on researches made by French and Belgian scientists as well as Russian and Ukrainian researches.

The author used methods of comparative law, historical method, method of induction, system-structural method, formal-logical method and other methods of scientific research. Rights, obligations and responsibility of electronic trust services providers are considered in this article. Special attention is payed to the analysis of, differences between the legal status of qualified and non-qualified providers. The author proposed classification of parties of legal relations in the field of electronic identification and electronic trust services.

The author explains why regulatory measures are mostly applied to qualified providers rather than non-qualified. Advantages of using services provided by qualified providers, in particular several presumptions are considered.

Results of the research may be used in judicial proceedings where electronic documents are examined. Moreover, it can be used while drafting government rules and regulations in the field of electronic trust services.

Key words: electronic trust services, provider of electronic trust services, electronic identification, electronic signature.