Пузиренко Олександр Юрійович, кандидат технічних наук, доцент кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: ajiekc1980@gmail.com
Пузыренко Александр Юрьевич, кандидат технических наук, доцент кафедры телекоммуникационных систем Национального авиационного университета.
Puzyrenko Alexander, PhD in Eng., associate professor of Academic Department of Telecommunication systems, National Aviation University.

Андрухович Петро Олександрович, старший викладач кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: peter.andrukhovich@gmail.com

Андрухович Петр Александрович, старший преподаватель кафедры телекоммуникационных систем Национального авиационного университета.
Andrukhovich Petr, Senior Lecturer of Academic Department of Telecommunication systems, National Aviation University.

Терентьєва Ірина Євгенівна, аспірант кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: i.terentyeva@ukr.net
Терентьева Ирина Евгеньевна, аспирант кафедры телекоммуникационных систем Национального авиационного университета.
Terentyeva Irina, postgraduated student of Academic Department of Telecommunication systems, National Aviation University.

УДК 681.3. 06 (07)

СУТНІСТЬ ЗАКОНОДАВЧИХ ОСНОВ ТА УМОВИ НАДАННЯ ДОВІРЧИХПОСЛУГ В ЕВРОПЕЙСЬКОМУ СОЮЗІ В ПЕРІОД 2015 – 2030 рр.

Юрій Горбенко

Розглядаються питання стану та необхідності удосконалення нормативно – правової законодавчої бази Європейського союзу (ЄС) відносно електронних довірчих операцій на внутрішньому ринку. Аналізуються основні положення "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку". Робиться висновок про актуальність та необхідність приєднання України до електронного цифрового ринку ЄС та проведення відповідних досліджень та виконання розробок. Аналізується стан впровадження інфраструктури відкритого ключа, а в Україні системи ЕЦП, на практиці. Наводяться основні проблемні питаннями, що виникли в процесі застосування ЕЦП, - уніфікації, стандартизації, сумісності, масштабуємості, криптографічної стійкості, складності криптографічних перетворень тощо. Розробляються пропозиції, а також визначається сутність та визначаються умови відносно прийняття основних положень Регламенту для практичної реалізації, в тому числі на перспективу в Україні. Визначаються вимоги, які повинні бути вирішені в ЄС для надання безпечних електронних послуг щодо електронної ідентифікації, електронної автентифікації, електронного підпису, електронних печаток, електронних міток часу, електронних документів, послуг електронної доставки та перевірки справжності веб – сайту.

Ключові слова: *електронний цифровий ринок ЄС, електронні операції, механізми ідентифікації, автентифікації та електронні довірчі послуги.*

ВСТУП

Початок XXI століття характеризується інтенсивним впровадження інфраструктур відкритого ключа (ІВК) на практиці, основними завданнями яких стало виготовлення та обслуговування сертифікатів відкритих ключів для асиметричних криптографічних перетворень типу (електронний) цифровий підпис та направлений шифр [1, 2, 9]. Такі інфраструктури в основному є третіми довіреними сторонами. В Україні ІВК отримала назву системи електронного цифрового підпису (ЕЦП) [4]. Зрозуміло, що створення та застосування ІВК безпосередньо пов'язані з їх законодавчим та нормативно-правовим забезпеченнями. Історично спочатку в США [10], а потім і в ЄС [3] приймається закон (директива) та необхідний перелік нормативно-правових документів, що стосуються застосування (електронного) цифрового підпису та направленого шифрування. До того, як у 2000 р. президент США підписав закон «Про електронний цифровий підпис», практично в усіх штатах США він уже діяв, наприклад закон штату Юта «Про електронний цифровий підпис» був прийнятий в 1996 р. В

Германії закон «Про електронний цифровий підпис «прийнятий в 1997 р. Згодом в РФ [8] і Україні під певним впливом [3, 8] також приймається закон [4] та Правила посиленої сертифікації, що стосуються ЕЦП [7]. Внаслідок ЕЦП став обов'язковим механізмом, з використанням якого в інформаційно-телекомунікаційних системах забезпечується надання таких базових послуг як цілісність, справжність, неспростовність відправника (авторство) електронних даних, повідомлень тощо. Нині у світі використовується сотні мільйонів сертифікатів відкритих ключів, в тому числі значно більше мільйона в Україні.

Основними проблемними питаннями, що виникли в процесі застосування ЕЦП, є питання уніфікації, стандартизації, сумісності, масштабуємості, криптографічної стійкості, складності криптографічних перетворень, а також відповідність значному числу інших вимог [1-3, 6-7]. Їх вирішення здійснювалось на основі міжнародної, національної та регіональної стандартизації алгоритмів ЕЦП, внаслідок чого з'явилось значне число, як правило, несумісних стандартів та механізмів [1-2]. В Україні для вирішення значного числа вказаних протиріч були прийняті закони України [5, 6]. Ще складнішими стали питання уніфікації технічних специфікацій форматів даних [1, 2] тощо, їх реалізації з забезпеченням захищеності від компрометації особистих ключів та компрометації засобів криптографічного захисту в цілому.

Внаслідок вказаного знову з'явилось десятки національних чи регіональних стандартів, наприклад в ЄС. В той же час визнано, що зміцнення довіри у он-лайн середовищі є ключем до економічного розвитку [11]. Відсутність довіри змушує споживачів, бізнес і керівництво коливатися при здійсненні операцій в електронному вигляді та приймати нові послуги. Тому в ЄС визнано ряд існуючих обмежень відносно електронного (цифрового) розвитку Європи і запропоновано новітнє законодавство про електронні підписи, взаємне визнання електронної ідентифікації та електронної автентифікації, а також необхідність розроблення та прийняття чіткої законодавчої бази, забезпечення сумісності, підвищення використання громадянами електронних систем та суттєвого запобігання кіберзлочинності. Необхідність вирішення вказаних задач є необхідною умовою реалізації єдиного електронного ринку, що уже закріплено в Акті про Єдиний Ринок ЄС [11]. Вказане вимагає запровадження в ЄС законодавства, яке забезпечувало б взаємне визнання електронної ідентифікації та автентифікації на всій території ЄС, а також вирішити протиріччя, що закладені в положеннях Директиви про електронні цифрові підписи [5]. Особливо важливим є взаємне визнання та прийняття електронної ідентифікації та автентифікації не зважаючи на кордони.

Запропонована законодавча база, що складається з "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку", призначена забезпечити безпечні і цілісні електронні операції між підприємствами, громадянами і державними органами, що дозволить підвищити ефективність державних і приватних онлайн-послуг, електронного бізнесу та електронної торгівлі в ЄС. Діюче чинне законодавство ЄС, тобто Директива 1999/93/ЄС про "Загальні основи для електронних підписів", в основному охоплює тільки електронні підписи. Таким чином визнано, що в ЄС нині не існує всебічних транскордонних та міжрегіональних основ для безпечних, надійних і простих електронних операцій, включаючи електронну ідентифікацію, електронну автентифікацію та електронні цифрові підписи. У цілому основною метою прийняття "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку" є покращення існуючого законодавства і його розширення для забезпечення взаємного визнання і прийняття на рівні ЄС заявлених електронних механізмів ідентифікації, автентифікації та інших необхідних електронних довірчих послуг.

Метою цієї статі є визначення проблемності та актуальності, аналізу та розробки пропозицій, а також визначення умов відносно прийняття основних положень Регламенту [1] для практичної реалізації, в тому числі на перспективу в Україні.

1. СТАН ТА НЕОБХІДНІСТЬ УДОСКОНАЛЕННЯ ЗАКОНОДАВЧОЇ БАЗИ ЄС ВІДНОСНО ЕЛЕКТРОННИХ ОПЕРАЦІЙ.

В наслідок практичного застосування ЕЦП в ЄС, поряд з позитивним досвідом, виявлене певне число протиріч та недоліків. В першу чергу виявлено багато фактів недовіри до електронних операцій на внутрішньому ринку ЄС. Також визнано, що зміцнення довіри у он-лайн-середовищі є ключем до економічного розвитку, так як відсутність довіри змушує споживачів, бізнес і керівництво обережно відноситись до здійснення операцій в електронному вигляді, особли-

во приймати нові послуги. Проблемними виявились питання, що стосуються електронних підписів, взаємного визнання електронної ідентифікації та електронної автентифікації, наявність необгрунтованої фрагментації та несумісності, не достатня активність громадян в застосуванні електронних послуг, а також недопустимий рівень кіберзлочинності. Вирішення вказаних протиріч в першу чергу пов'язане з розробкою, широким обговоренням та прийняттям необхідних нормативно-правових актів. Тобто законодавство, яке забезпечить взаємне визнання електронної ідентифікації та електронної автентифікації на всій території ЄС, а також переглядає положення Директиви про електронні підписи [5] є основоположною дією для реалізації єдиного цифрового ринку ЄС. Особливістю такого законодавства є взаємне визнання і прийняття електронної ідентифікації і автентифікації, не зважаючи на існуючі кордони. Законодавча база, що запропонована, складається з "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку" [11, 12], призначена забезпечити безпечність та цілісність електронні операції між підприємствами, громадянами і державними органами. Законодавство, що є чинним в ЄС, тобто Директива 1999/93/ЄС про "Загальні основи для електронних підписів", в основному охоплює тільки електронні підписи. Тому можна стверджувати, що в ЄС відсутні всебічні можливості для здійснення транскордонних та міжрегіональних безпечних, надійних і простих електронних операцій, що включають електронну ідентифікацію, автентифікацію та електронні підписи. Метою удосконалення законодавства є покращення існуючого законодавства і його розширення для забезпечення взаємного визнання і прийняття на рівні ЄС заявлених електронних схем ідентифікації, електронної автентифікації та інших довірчих послуг (eIAS).

Аналіз підходів до вирішення вказаних вище завдань показав, що вони базуються на демократичних принципах. Запропонований регламент є результатом широких нарад за участі членів ЄС, в ході цих нарад Комісія зібрала відгуки державчленів Європейського парламенту та інших зацікавлених сторін. В розробці Регламенту активність проявив малий та середній бізнес. Детально матеріали нарад можна знайти в [12]. Комісія, що булла створена в ЄС, також запустила ряд досліджень щодо електронної ідентифікації, автентифікації, електронного підпису та пов'язаних з ними довірчих послуг. В ході нарад стало зрозумілим, що більшість зацікавлених сторін погодилися відносно перегляду існуючої законодавчої бази. Це дозволяє заповнити прогалини, що залишені в результаті реалізації Директиви про електронні підписи [5]. Також висловлено думку, що треба ефективніше та оперативніше реагувати на виклики, що кинуті швидким розвитком нових технологій, зокрема, он-лайн доступу і мобільності доступу, а також зростанням глобалізації.

В результаті роботи комісії були оцінені три набори варіантів політики, що відносяться відповідно до сфери: застосування нормативної нової бази; законодавчого інструменту та необхідного рівню контролю. В якості найбільш прийнятного визнано варіант політики, який спрямований на підвищення правової визначеності, покращення координації з боку національного контролю, забезпечення взаємного визнання і прийняття схем електронної ідентифікації та введення важливих довірчих послуг. Також в ході оцінювання було визнано, що виконання вищезазначеного може призвести до значного поліпшення правової визначеності, рівня безпеки та довіри до транскордонних електронних операцій. Вказане також призведе до зменшення фрагментації ринку.

2. СУТНІСТЬ ЗАКОНОДАВЧИХ ЕЛЕМЕНТІВ РЕГЛАМЕНТУ.

Законодавчі елементів Регламенту призначені для усунення існуючих бар'єрів функціонування внутрішнього ринку в ЄС. При їх впровадженні громадяни, підприємства і керівництво зможуть отримати користь від взаємного визнання і прийняття електронної ідентифікації, електронної автентифікації, електронних підписів та інших довірчих послуг, не зважаючи на кордони. В ЄС визнано, що Регламент є найбільш підходящим правовим документом. При цьому безпосереднє застосування правил Регламенту знизить законодавчу фрагментацію і забезпечить більшу правову визначеність шляхом введення погодженого набору основних правил, введених в дію на внутрішніх ринках держав-членів ЄС.

Аналіз показує, що основними принципами, що закладені в Регламенті є принципи додатковості та тестування ефективності. Сутність принципу додатковості зводиться до розгляду транс національних завдань та рішучих дій, тому що тільки внутрішні, тобто на національному рівні дії самі по собі не є достатніми для досягнення цілей. Тоді як досвід свідчить про те, що існуючі національні заходи вже створили перешкоди на шляху загальноєвропейської взаємодії в частині

електронних підписів. Якраз вони нині мають суттєвий вплив на вирішення проблем електронної ідентифікації, електронної автентифікації та пов'язаних з ними довірчих послуг. Тому важливо, щоби ЄС створив сприятливу основу для вирішення проблем транскордонної взаємодії та покращення координації національних систем контролю. В той же час проведений аналіз показав, що проблема електронної ідентифікації не може бути вирішена в запропонованому Регламенті тим же загальним способом, як для інших електронних довірчих послуг. Це пов'язане з тим, що випуск засобів ідентифікації нині є національною прерогативою. Тому пропозиція в значній мірі зосереджена винятково на транскордонних аспектах електронної ідентифікації. Розроблений та запропонований Регламент створює рівні умови для підприємств, що надають довірчі послуги. В даний час існуючі відмінності в національних законодавствах часто призводить до правової невизначеності і додаткових обмежень. Також правова визначеність з указаного питання значно поліпшиться за рахунок прийняття державами-членами чітких зобов'язань щодо кваліфікованих довірчих послуг. Вказане створить додаткові стимули для виходу бізнесу за кордон. Так, компанії зможуть брати участь у тендері електронно, що оголошені керівництвом іншої держави-члена без проблем блокування електронного підпису у зв'язку з конкретними національними вимогами і проблемами з сумісністю. Крім того, компанії зможуть підписувати контракти з партнерами в електронному вигляді, не боячись різних правових вимог до довірчих послуг, таких як електронні пломби, електронні документи або відмітки часу. Крім того усі повідомлення про невиконання будуть доставлені з однієї держави-члена до іншої і матимуть юридичну силу в обох державах-членах ЄС. Також торгівля через internet буде більш надійною, коли покупці матимуть засіб, щоб переконатися, що вони дійсно зайшли на сайт обраного продавця, а не на підроблений веб-сайт.

Важливим є взаємне визнання електронних засобів ідентифікації. Якраз широко прийняті електронні підписи будуть сприяти транскордонному наданню численних послуг на внутрішньому ринку і дозволять бізнесу вийти за кордон, не стикаючись з перешкодами при взаємодії з органами державної влади. Практично це дозволить значно підвищити ефективність як для підприємств, так і громадян, за умови дотримання адміністративних формальностей. Наприклад, це дасть можливість студенту вступити електронним способом до університету за кордоном, громадянину – представити он-лайн податкову декларацію іншій державі-члену або пацієнту отримати доступ до своїх медичних даних в режимі он-лайн. Якщо таких взаємно визнаних електронних засобів ідентифікації не буде, то лікар не зможе отримати доступ до медичних даних пацієнта, що необхідні для його лікування. Крім того медичні та лабораторні аналізи, які пацієнт вже пройшов, доведеться робити знову.

Цілі, що викладені вище, нині не досягаються за рахунок відсутності добровільної координації між державами-членами ЄС, і малоймовірно, що воно відбудеться в майбутньому. Тому в державах здійснюється дублювання робіт, використовуються різні стандарти, а також виникають адміністративні складності при координації шляхом двосторонніх і багатосторонніх угод. Крім того, існує необхідність вирішення протиріч, що пов'язані з відсутність правової визначеності відносно національних положень, які випливають з різних тлумачень Директиви про електронні підписи, а також відсутність сумісності систем електронного підпису, що використовується на національному рівні. Тому є необхідність координації дій відносно застосування технічних стандартів та форматів даних, яка на рівні ЄС була б більш ефективною.

3. АНАЛІЗ ОСНОВНИХ ПОЛОЖЕНЬ ПРОПОЗИЦІЙ ВІДНОСНО РЕГЛАМЕНТУ

Основні положення Регламенту викладені у вигляді 42 статей.

Стаття 1 визначає предмет, а стаття 2 визначає сферу дії Регламенту. Стаття 3 містить визначення термінів. Деякі з визначень узяті з Директиви 1999/93/ЄС, інші були уточнені, доповнені додатковими елементами, або нововведеними. В статі 4 визначає принципи внутрішнього ринку, грунтуючись на територіальному застосуванні Регламенту. Причому основоположним є відсутність будь-яких обмежень на свободу надання послуг і вільного обігу продукції.

3.1. Електронна ідентифікація.

Статі 5-8 присвячені електронній ідентифікації. В них передбачається взаємне визнання і прийняття засобів електронної ідентифікації, що підпадають під схему(механізм), яка буде представлена кожною державою Комісії згідно умов, що наведені в Регламенті. При цьому більшість держав-членів ЄС уже ввели деякі форми електронної системи ідентифікації, які відрізняються в багатьох аспектах. Але відсутність загальної пра-

вової бази, що вимагала б від кожної держави-члена визнавати і приймати електронні засоби ідентифікації, що випущені іншими державами-членами для доступу до онлайн-послуг, створює бар'єри, що перешкоджають громадянам і підприємствам користуватися всіма перевагами єдиного електронного цифрового внутрішнього ринку. Тому взаємне визнання і прийняття будь-яких електронних засобів ідентифікації, що підпадають під представлену державою схему на підставі Регламенту знищує існуючі правові бар'єри. При цьому Регламент не зобов'язує держави-члени вводити або повідомляти про схеми електронної ідентифікації, але зобов'язує визнати і прийняти представлену електронну ідентифікацію для тих он-лайн послуг, де електронна ідентифікація необхідна щоб отримати доступ на національному рівні. Але, можливе зростання економіки за допомогою транскордонного використання представлених електронних засобів ідентифікації і систем автентифікації, може стимулювати держав-членів повідомляти про свої схеми електронної ідентифікації.

Стаття 6 Регламенту встановлює визначає чотири умови для представлення електронних схем ідентифікації.

1) Держави-члени ЄС можуть представляти схеми електронної ідентифікації, які вони прийняли під своєю юрисдикцією для випадків, коли електронна ідентифікація необхідна для громадських послуг. Іншою вимогою є те, що відповідні електронні засоби ідентифікації повинні бути випущені від імені або принаймні під відповідальність держави, що представляє схему.

2) Держави-члени повинні забезпечити однозначний зв'язок між електронними ідентифікаційними даними і особою, до якої вони відносяться. Ця вимога не означає, що особа не може мати кілька електронних засобів ідентифікації, але всі вони повинні пов'язуватися з нею.

3) Надійність електронної ідентифікації повинна залежати від доступності засобів автентифікації, тобто можливості перевірити достовірність електронних ідентифікаційних даних. Держави-члени ЄС повинні забезпечити он-лайн автентифікацію для третіх сторін безкоштовно. При цьому автентифікація повинна бути доступна безперервно і ніякі конкретні технічних вимоги, наприклад такі як апаратне або програмне забезпечення, не можуть пред'являтись сторонам відносно здійснення автентифікації. Але ця вимога не поширюється на будь-які вимоги по відношенню до користувачів (власників) електронних засобів ідентифікації, які є технічно необхідними для використання електронних засобів ідентифікації, наприклад таких як зчитувачі карт.

4) Держави-члени ЄС повинні взяти на себе відповідальність за однозначність їх зв'язку з особою, тобто, що вони не пов'язані з будь-якою іншою особою. Також повинна існувати можливість їх автентифікації, тобто перевірити достовірність електронних ідентифікаційних даних. При цьому відповідальність держав-членів не поширюється на інші аспекти процесу ідентифікації або будь-яких операцій, які вимагаються при виконанні ідентифікації.

Стаття 7 Регламенту містить правила представлення Комісії схем електронної ідентифікації, а стаття 8 вказує на необхідність забезпечення технічної сумісності представлених схем ідентифікації шляхом координації.

3.2. Довірчі послуги.

Статті 9-37 присвячені довірчим послугам, причому статі 9-12 містять загальні положення, 13-19 питання нагляду, 20-27 питання електронного підпису, 28-31 електронної печатки, 32-33 електронної мітки часу, 34 – електронні документи, 35-36 послуги електронної доставки, 37 – автентифікації сайту. Розглянемо сутність та вимоги до вказаних вище послуг біль детальніше.

Загальні положення. Стаття 9-12 встановлює принципи, що стосуються відповідальності як некваліфікованих, так і кваліфікованих провайдерів довірчих послуг. Вона ґрунтується на статті 6 Директиви 1999/93/ЄС [6] та поширює право на відшкодування збитків, заподіяних некомпетентним провайдером довірчих послуг. Основою відшкодування збитків служить доведене нехтування забезпеченням відповідного рівня захисту, що призводять до порушення безпеки. Далі, в стаття 10 описується механізм визнання і прийняття кваліфікованих довірчих послуг, наданих провайдером, розташованим в іншій країні. В свою чергу він ґрунтується на статті 7 Директиви 1999/93/ЄС, але в регламенті збережено тільки один практичний варіант, який дозволяє визнання факту в рамках міжнародної угоди між Європейським Союзом та іншими країнами чи міжнародними організаціями. В статті 11 викладені принцип захисту і мінімізації даних, він ґрунтується на статті 8 Директиви 1999/93/ЄС. В статі 12 викладаються особливості надання довірчих послуг інвалідам.

Здійснення нагляду. Особливістю нагляду є те, що згідно статті 13 держави-члени ЄС зобов'язані на підставі статті 3 Директиви 1999/93/ЄС ство-

рити наглядові органи. При цьому необхідно уточнити та розширити їх повноваження по відношенню до провайдерів довірчих послуг та кваліфікованих провайдерів довірчих послуг. В статті 14 для полегшення транскордонного контролювання провайдерів довірчих послуг наведено явний механізм взаємної допомоги між наглядовими органами в державах-членах. Також пропонуються правила спільної діяльності та право участі наглядових органів в такій діяльності. В статі 15 вказується на обов'язкові для кваліфікованих і некваліфікованих провайдерів довірчих послуг відповідні технічні та організаційні заходів щодо забезпечення безпеки їх діяльності. Також вимагається щоби компетентні наглядові органи та інші відповідні органи повинні бути поінформовані про будь-які порушення безпеки. При необхідності, вони у свою чергу інформують наглядові органи інших держав-членів і, безпосередньо, або через відповідного постачальника довірчих послуг, а також інформують громадськість. В статті 16 викладаються вимоги відносно нагляду за кваліфікованими провайдерами довірчих послуг і кваліфікованими довірчими послугами, які надаються ними. Згідно вимог кваліфіковані провайдери довірчих послуг зобов'язані щорічно проходити перевірку, яка виконується визнаним незалежним органом, щоб надати підтвердження наглядовому органу, що вони виконують зобов'язання, викладені в Регламенті. Також згідно статі 16 наглядовому органу надається право здійснювати безпосередньо на місці аудит кваліфікованих провайдерів довірчих послуг в будь-який час. Наглядовий орган також має право видавати для кваліфікованих провайдерів довірчих послуг обов'язкові для виконання інструкції, призначенням яких є виправлення невиконаних ним вимог безпеки. В статті 17 викладається порядок перевірки та допуску наглядовим органом провайдерів кваліфікованих довірчих до надання ним довірчих послуг. В статті 18 викладаються вимоги до порядку створення довірених списків, які містять інформацію про кваліфікованих провайдерів довірчих послуг. Вони якраз і є суб'єктами нагляду та кваліфікованих послуг, які вони пропонують. Вказана інформація про кваліфікованих провайдерів довірчих послуг повинна бути піддана гласності, щоб полегшити її автоматизоване використання і забезпечити належний рівень деталізації. Нарешті в статті 19 встановлюються вимоги до кваліфікованих провайдерів довірчих послуг, яким вони повинні відповідати, щоб бути визнаними кваліфікованими. Стаття ґрунтується на Додатку II Директиви 1999/93/ЄС.

Електронний підпис. В статті 20 Регламенту викладаються правила, що пов'язані з юридичним визнанням електронних підписів фізичних осіб. По суті вона уточнює і розширює статтю 5 Директиви 1999/93/ЄС та вводить чіткі зобов'язання надати кваліфікованим електронним підписам таку ж юридичну силу, як і ручним (на бумазі) підписам. Також держави-члени ЄС повинні забезпечити для надання громадських послуг транскордонне прийняття кваліфікованих електронних підписів. Також не повинні вводитись ніякі додаткові вимоги, які можуть створювати бар'єри на шляху використання таких електронних підписів. Далі в статті 21 викладені вимоги для сертифікатів кваліфікованого підпису. По суті в ній уточнюється додаток I Директиви 1999/93/ЄС. Також відкликаються положення, які не застосовуються на практиці, наприклад, обмеження на вартість операції.

В статті 22 Регламенту викладаються вимоги до пристроїв вироблення кваліфікованих електронних підписів. Уточняються вимоги до захищених пристроїв для створення підписів, що викладені в статті 3 Директиви 1999/93/ЄС. Вони повинні розглядатися в якості пристроїв створення кваліфікованого підпису у відповідності з Регламентом, що пропонується. Також визначається, що сфера використання пристроїв для створення підпису може бути набагато ширшою. Згідно цієї статті Комісія може також скласти та рекомендувати список відповідних стандартів щодо вимог безпеки до пристроїв. В статті 23 на основі статті 3 (4) Директиви 1999/93/ЄС, вводиться поняття сертифікації пристроїв кваліфікованого електронного підпису. Вона вводиться з метою визначення їх відповідності вимогам безпеки, що викладені у додатку II Директиви 1999/93/ЄС. Вказані пристрої повинні бути визнані всіма державами-членами як такі, що відповідають вимогам, якщо процедура сертифікації проводиться органом з сертифікації, призначеним державою-членом. За виконання вказаних вимог Комісія буде публікувати перелік таких сертифікованих пристроїв. Комісія може також скласти та використовувати для оцінки безпеки продуктів інформаційних технологій список стандартів, що зазначені у статті 23. Стаття 24 безпосередньо стосується публікації Комісією списку пристроїв створення кваліфікованого електронного підпису після повідомлення державами-членами про їх відповідність. В статті 25 з метою підвищення

правової визначеності перевірки кваліфікованих електронних підписів викладені обов'язкові вимоги, які ґрунтується на рекомендаціях Додатку IV Директиви 1999/93/ЄС щодо. В статті 26 викладені вимоги відносно перевірки кваліфікованих послуг електронного підпису, причому кваліфікована послуга перевірки для кваліфікованих електронних підписів повинна надаватись кваліфікованим провайдером довірчих послуг. Стаття 27 визначає вимоги відносно довгострокового збереження кваліфікованих електронних підписів. Для цього повинні використовуватись процедури, механізми і технології, з використанням яких можна продовжити після закінчення часу їх технологічної придатності, термін їх дійсності, але за умови що за цей кібер злочинці можуть зробити підробку ключових даних.

Електронні печатки. В статті 28 Регламенту викладаються вимоги та умови відносно юридичної сили електронних печаток юридичних осіб. Відносно конкретні правові презумпції можуть надаватись лише кваліфікованій електронній печатці, яка гарантує походження і цілісність електронних документів, що нею завірені. В статті 29 викладаються вимоги до кваліфікованих сертифікатів для електронних печаток. Так вони повинні відповідати вимогам, що наведені в додатку III до Регламенту. В статті 30 викладаються вимоги до процедур сертифікації та публікації списку пристроїв, які можуть бути використані для створення кваліфікованих електронних печаток. Нарешті, в статі 31 викладені вимоги відносно перевірки та збереження кваліфікованих електронних печаток. Вони ґрунтуються на статтях 25-27 Регламенту з відповідними змінами у порівнянні з електронними підписами.

Електронна мітка часу. Стаття 32 Регламенту стосується забезпечення юридичної сили електронних міток часу. При цьому конкретні правові презумпції надаються кваліфікованим електронним міткам часу з вимогою забезпечення певної точності часу. В статті викладаються вимоги відносно кваліфікованих електронних міток часу.

Електронні документи. В статті 34 Регламенту викладені вимоги та умови забезпечення юридичної сили визнання електронних документів. Також визначаються певні правові презумпції автентичності та цілісності будь-якого електронного документа, що зроблений з використанням кваліфікованого електронного підпису або такого, що скріпленого кваліфікованою електронною печаткою. При цьому електронні документи, що видані особами, компетентними відносно видачі відповідних документів і які вважаються оригіналами або їх завіреними копіями відповідно до національного законодавства держави-члена, повинні бути прийняті в інших державах-членах без додаткових вимог.

Послуги електронної доставки. В статті 35 викладаються вимоги відносно юридичної сили даних, що надіслані або отримані за допомогою послуг електронної доставки. При цьому конкретні правові презумпції щодо цілісності даних, які відправлені чи отримані, і точність часу, в який дані відправлені або отримані, гарантується кваліфікованою послугою електронної доставки. В статті також визначаються вимоги відносно взаємного визнання кваліфікованих послуг електронної доставки на рівні ЄС. В статті 36 визначені вимоги для кваліфікованих послуг електронної доставки.

Автентифікація сайту. Ця послуга призначена для того, щоб забезпечити справжність веб-сайту і вона була гарантована власником сайту. Далі, в статті 37 викладені вимоги до кваліфікованих сертифікатів автентифікації веб-сайту, які можуть бути застосовані для того, щоб гарантувати справжність веб-сайту. При цьому кваліфікований сертифікат автентифікації веб-сайту повинен надавати мінімальну кількість достовірної інформації про веб-сайт та про легальне існування свого власника.

3.3. Делеговані акти та реалізація актів.

В регламенті також визначені питання, що стосуються можливостей Комісії відносно певних актів, що не носять законодавчого характеру. Так стаття 38 містить стандартні положення щодо здійснення такого делегування. Це дозволяє законодавцю делегувати Комісії повноваження приймати не законодавчі акти загального застосування, щоб доповнити або змінити певні несуттєві елементи законодавчого акту.

Що стосується реалізація актів, то відповідні положення Регламенту визначають процедури та можливості Комісії при її діяльності. Так стаття 39 містить положення, які визначають процедури Комісії, що необхідні для реалізації її повноважень, які закріплені для виконання юридично визнаних актів ЄС. Також може застосовуватись процедура експертизи.

3.4 Прикінцеві положення та бюджетні питання.

Прикінцеві положення. В параграфі прикінцевих положень викладені питання необхідності, чи навіть обов'язки Комісії відносно вивчення та аналізу Регламенту. Так згідно статті Комісія зобов'язана оцінити Регламент і доповісти про свої

висновки. Дуже важливе є те, що в статті 41 вказується про скасування Директиви 1999/93/ЕС і про необхідність забезпечення плавного переходу від існуючої інфраструктури електронного підпису до нових вимог Регламенту. Стаття 42 встановлює дату набуття чинності цього Регламенту, так він згідно статті набуває чинності на 20 день після його опублікування в офіційному журналі ЄС.

Бюджетні питання. Законодавчі фінансові постанови, що супроводжують цю пропозицію відносно Регламенту поширюються на бюджетні питання самого Регламенту. Конкретні бюджетні питання цієї пропозиції відносно впровадження Регламенту пов'язані з завданнями, що покладені на Європейську комісію. Вона повинна діяти у відповідності до того як зазначено в законодавчих фінансових постановах, супроводжуючих пропозицію Регламенту. Пропозиція відносно цього Регламенту не має наслідків для поточних витрат.

4. ВИСНОВКИ ТА ПРОПОЗИЦІЇ ВІДНОСНО РЕГЛАМЕНТУ ТА ЙОГО ЗАСТОСУВАННЯ В УКРАЇНІ.

Проведений аналіз пропозицій, що містяться в Регламенті, дозволяє зробити такі основоположні висновки, оцінки та пропозиції.

В ЄС визнано, що зміцнення довіри у онлайн-середовищі є ключем до економічного розвитку [11]. Відсутності довіри змушує споживачів, бізнес і керівництво коливатися при здійсненні операцій в електронному вигляді та приймати нові послуги. Також в ЄС визначено ряд існуючих обмежень відносно електронного (цифрового) розвитку Європи і запропоновано новітнє законодавство про електронні підписи, взаємне визнання електронної ідентифікації та електронної автентифікації, а також необхідність розроблення та прийняття чіткої законодавчої бази, забезпечення сумісності, підвищення використання громадянами електронних систем та суттєвого запобігання кіберзлочинності. Необхідність вирішення вказаних задач є необхідною умовою реалізації єдиного електронного ринку, що уже закріплено Акті про Єдиний Ринок 2 ЄС [11]. Вказане вимагає запровадження в ЄС законодавства, яке забезпечувало б взаємне визнання електронної ідентифікації та автентифікації на всій території ЄС, а також вирішили протиріччя, що закладені в положеннях Директиви про електронні цифрові підписи [6]. Особливо важливим є взаємне визнання та прийняття електронної ідентифікації та автентифікації не зважаючи на кордони.

2. Пропозиція відносно "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку" є основоположним перспективним нормативно-правовим документом, який по суті розроблений на основі досвіду створення, застосування та удосконалення інфраструктури відкритого ключа ЄС і направлений на забезпечення безпечних, цілісних електронних операції між підприємствами, громадянами і державними органами. Його впровадження дозволить підвищити ефективність державних і приватних онлайн-послуг, електронного бізнесу та електронної торгівлі в ЄС.

3. Нині діюче чинне законодавство ЄС, тоб то Директива 1999/93/ЄС про "Загальні основи для електронних підписів", в основному охоплює тільки електронні підписи і не відповідає новітнім вимогам зі сторони електронного ринку ЄС. Регламентом визнано, що в ЄС нині не існує всебічних транскордонних та міжрегіональних основ для безпечних, надійних і простих електронних операцій, включаючи електронну ідентифікацію, електронну автентифікацію та електронні цифрові підписи.

4. Основною метою прийняття "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку" є покращення існуючого законодавства і його розширення для забезпечення взаємного визнання і прийняття на рівні ЄС заявлених електронних механізмів ідентифікації, автентифікації та інших необхідних електронних довірчих послуг.

5. Основними проблемними питаннями, що виникли в процесі застосування в ЄС ЕЦП, стали питання уніфікації, стандартизації, сумісності, масштабує мості, криптографічної стійкості, складності криптографічних перетворень тощо. Вирішення вказаних проблемних питань здійснювалось на основі міжнародної, національної та регіональної стандартизації ЕЦП, внаслідок неузгоджених дій в указаному напряму з'явилось значне число, як правило, несумісних стандартів та механізмів.

6. В ході практичного застосування ЕЦП в ЄС виявлене певне число протиріч та недоліків, в першу чергу багато фактів недовіри до електронних операцій на внутрішньому ринку ЄС. Визнано, що зміцнення довіри у он-лайн-середовищі є ключем до економічного розвитку, так як відсутність довіри змушує споживачів, бізнес і керівництво обережно відноситись до здійснення опера-

цій в електронному вигляді, особливо приймати нові послуги. Проблемними виявились питання, що стосуються електронних підписів, взаємного визнання електронної ідентифікації та електронної автентифікації, наявність необґрунтованої фрагментації та несумісності, не достатня активність громадян в застосуванні електронних послуг, а також недопустимий рівень кіберзлочинності. Вирішення вказаних протиріч в першу чергу пов'язане з розробкою, широким обговоренням та прийняттям необхідних нормативно-правових актів. Особливістю такого законодавства є взаємне визнання і прийняття електронної ідентифікації і автентифікації, не зважаючи на існуючі кордони.

7. Законодавча база ЄС, що запропонована, складається з "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку". Вона призначена забезпечити безпечність та цілісність електронні операції між підприємствами, громадянами і державними органами.

8. Директива 1999/93/ЄС про "Загальні основи для електронних підписів", в основному охоплює тільки електронні підписи. Тому можна стверджувати, що в ЄС відсутні всебічні можливості для здійснення транскордонних та міжрегіональних безпечних, надійних і простих електронних операцій, що включають електронну ідентифікацію, автентифікацію та електронні підписи. Метою удосконалення законодавства є покращення існуючого законодавства і його розширення для забезпечення взаємного визнання і прийняття на рівні ЄС заявлених електронних схем ідентифікації, електронної автентифікації та інших довірчих послуг.

9. Аналіз підходів до вирішення вказаних протиріч показав, що запропонований Регламент є результатом широких нарад за участі членів ЄС, в ході цих нарад Комісія зібрала відгуки державчленів Європейського парламенту та інших зацікавлених сторін. В розробці Регламенту активність проявив малий та середній бізнес.

10. Комісія, що булла створена в ЄС, також запустила ряд досліджень щодо електронної ідентифікації, автентифікації, електронного підпису та пов'язаних з ними довірчих послуг. При проведенні нарад стало зрозумілим, що більшість зацікавлених сторін погодилися відносно перегляду існуючої законодавчої бази. Вказане дозволяє заповнити прогалини, що залишені в результаті реалізації Директиви про електронні підписи [6]. Також визнано, що потрібно оперативніше реагувати на виклики, що виникли з швидким розвитком нових технологій, зокрема, он-лайн доступу і мобільності доступу, а також зростанням процесів глобалізації.

11. За результатами досліджень в якості найбільш прийнятного визнано варіант політики, який спрямований на підвищення правової визначеності, покращення координації з боку національного контролю, забезпечення взаємного визнання і прийняття схем електронної ідентифікації та введення важливих довірчих послуг. Це може призвести до значного поліпшення правової визначеності, рівня безпеки та довіри до транскордонних електронних операцій.

12. Основними принципами, що закладені в Регламенті є принципи додатковості та тестування ефективності. Сутність принципу додатковості зводиться до розгляду транс національних завдань та рішучих дій, тому що тільки внутрішні, тобто на національному рівні дії самі по собі не є достатніми для досягнення цілей. Тому важливо, щоби ЄС створив сприятливу основу для вирішення проблем транскордонної взаємодії та покращення координації національних систем контролю.

13. Проблема електронної ідентифікації не може бути вирішена в запропонованому Регламенті тим же загальним способом, як для інших електронних довірчих послуг. Вказане пов'язане з тим, що випуск засобів ідентифікації нині є національною прерогативою, а пропозиція в значній мірі зосереджена винятково на транскордонних аспектах електронної ідентифікації. Розроблений та запропонований Регламент створює рівні умови для підприємств, що надають довірчі послуги.

14. Існуючі відмінності в національних законодавствах часто призводить до правової невизначеності і додаткових обмежень. Також правова визначеність з указаного питання значно поліпшиться за рахунок прийняття державами-членами чітких зобов'язань щодо кваліфікованих довірчих послуг. Вказане створить додаткові стимули для виходу бізнес у за кордон.

15. Важливим є взаємне визнання електронних засобів ідентифікації. Якраз широко прийняті електронні підписи будуть сприяти транскордонному наданню численних послуг на внутрішньому ринку і дозволять бізнес у вийти за кордон, не стикаючись з перешкодами при взаємодії з органами державної влади.

16. Регламент ЄС не зобов'язує державичлени вводити або повідомляти про схеми елект-

ронної ідентифікації, але зобов'язує визнати і прийняти представлену електронну ідентифікацію для тих он-лайн послуг, де електронна ідентифікація необхідна щоб отримати доступ на національному рівні.

17. В статях 9-37 пропозицій Регламенту викладені вимоги до довірчих послуг, статті 9-12 містять загальні положення, 13-19 питання нагляду, 20-27 питання електронного підпису, 28-31 електронної печатки, 32-33 електронної мітки часу, 34 – електронні документи, 35-36 послуги електронної доставки, 37 – автентифікації сайту

18. В Регламенті також визначені питання, що стосуються можливостей Комісії, тобто певні акти(документи), що не носять законодавчого характеру. Важливим є принцип делегування Комісії повноваження приймати не законодавчі акти загального застосування.

19. Україна, при створенні національної системи ЕЦП при розробці закону "Про електронний цифровий підпис" [4] в якості основи використала Директиву [3]. Тому недоліки, що викладені відносно Директиви вище, в значній мірі відносяться і до існуючої національної системи ЕЦП.

20. У випадку інтеграції або ассоціації України в ЄС, все що викладене в Регламенті в повній мірі є актуальними і для України. Тим більше, що Україна в суттєвій мірі орієнтується на Європейський ринок. Зрозуміло, що при трансформації Європейського ринку в сторону електронного, потрібна така ж трансформація і в Україні, по крайній мірі на першому етапі для торгових відношень з Європою.

21. Наведені в цій статті результати аналізу та досліджень дозволяють зробити висновок та пропозиції відносно необхідності від слідкування та оцінки руху Європейського ринку до електронного, визначенні можливостей та умов розробки та прийняття відповідного законодавства та нормативно-правової бази і в Україні. За основу такої бази необхідно взяти Регламент [11].

22. Також потрібно вести значну роботу по пропоганді напряму удосконалення національного ринку в сторону електронного, тим більше, що в перспективі, при взаємодії з ЄС в Україні альтернативи немає.

23. В якості специфічного шляху розвитку цифрового світу можна навести приклад РФ, яка в 2011 р. ввела в дію Федеральний закон Російської Федерації "Об электронной подписи".

ЛІТЕРАТУРА

[1]. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Харків. Форт. 2010, 593 с.

[2]. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 878 с.

[3]. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства

[4]. Закон України «Про електронний цифровий підпис». № 852-IX від 22.05.2003

[5]. Закон України „Про електронний документ та електронний документообіг". №851-IV від 22.05.2003.

[6]. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". № 2594 – IV від 31.05.2005 р.

[7]. Правила посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 3 від 13.01.2005, зареєстрованих в Міністерстві юстиції України 27.01.2005 за № 104/10384 (у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 № 50).

[8]. Федеральний закон Российской Федерации «Об электронной цифровой подписи» от 10 января 2002 г.

[9]. Столлингс В. Криптография и защита сетей. Принципы и практика. Изд. "Вильямс". Киев. 2001. 669 с.

[10]. The Electronic Signatures in Global and National Commerce Act (ESIGN, Pub.L. 106-229, 14 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch.96. 106th Congress Public Law 229)

[11]. 11. Brussels, XXX. COM(2012) 238/2. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) {SWD(2012) 135} {SWD(2012) 136}.

[12]. http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

REFERENCES

[1]. Gorbenko Yu.I., Gorbenko I.D. Public Key Infrastructure. Systems EDS. Theory and Practice. Kharkiv. Fort. 2010, 593 p.

[2]. Gorbenko I.D., Gorbenko Yu.I.. Applied Cryptology. Monograph. Kharkiv, KNURE, Fort, 2012, 1st and 2nd edition, 878 p.

[3]. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on the

system of electronic signatures used in the Community.
[4]. The Law of Ukraine "On electronic digital signature". №852-IX of 22.05.2003.
[5]. The Law of Ukraine "On electronic document and electronic documents circulation". № 851-IV of 22.05.2003.
[6]. The Law of Ukraine "On Protection of Information in information - telecommunications systems." №2594 - IV of 31.05.2005.
[7]. Terms of qualified certification, approved by the Department of Special Telecommunication Systems and Information Protection of Security Service of Ukraine № 3 of 13.01.2005, registered by the Ministry of Justice of Ukraine of 27.01.2005 № 104/10384 (as amended by Order of the Department of Special Telecommunication Systems and Information Protection of Security Service of Ukraine of 10.05.2006 № 50).
[8]. Federal law of Russian Federation "On electronic digital signature" of 10 January 2002.
[9]. Stallings W. Cryptography and network security. Principles and practices. Pub. "Williams". Kiev. 2001. 669 p.
[10]. The Electronic Signatures in Global and National Commerce Act (ESIGN, Pub.L. 106-229, 14 Stat. 464, enacted June 30, 2000, 15 U.S.C. ch.96. 106th Congress Public Law 229).
[11]. Brussels, XXX. COM(2012) 238/2. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) {SWD(2012) 135} {SWD(2012) 136}.
[12]. http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision

СУЩНОСТЬ ЗАКОНОДАТЕЛЬНЫХ ОСНОВ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ ДОВЕРИТЕЛЬНЫХ УСЛУГ В ЕВРОПЕЙСКОМ СОЮЗЕ В ПЕРИОД 2015 – 2030 рр.

Рассматриваются вопросы состояния и необходимости совершенствования нормативно-правовой законодательной базы Европейского союза (ЕС) в отношении электронных доверительных операций на внутреннем рынке. Анализируются основные положения "Регламента Европейского Парламента и Совета по электронной идентификации и трастовых сервисов для электронных операций на внутреннем рынке". Делается вывод об актуальности и необходимости присоединения Украины к электронной цифровой рынке ЕС и проведения соответствующих исследований и выполнения разработок. Анализируется состояние внедрения инфраструктуры открытого ключа, а в Украине системы ЭЦП, на практике. Приводятся основные проблемные вопросы, возникшие в процессе применения ЭЦП, - унификации, стандартизации, совместимости, масштабируемости, криптографической стойкости, сложности криптографических преобразований и т.п. Разрабатываются предложения, а также определяется сущность и условия относительно принятия основных положений Регламента для практической реализации, в том числе на перспективу в Украине. Определяются требования, которые должны быть решены в ЕС для предоставления безопасных электронных услуг по электронной идентификации, электронной аутентификации электронной подписи, электронных печатей, электронных меток времени, электронных документов, услуг электронной доставки и проверки подлинности веб - сайта.

Ключевые слова: электронный цифровой рынок ЕС, электронные операции, механизмы идентификации, аутентификации и электронные доверительные услуги.

THE ESSENCE OF THE LEGAL FRAMEWORK AND CONDITIONS FOR THE PROVISION OF TRUST SERVICES IN THE EUROPEAN UNION IN THE PERIOD 2015 – 2030 pp.

The problems of the condition and the need to improve the regulatory and legal legislative base of the European Union (EU) for electronic trust operations in the domestic market are considered. The main provisions of the "Regulations of the European Parliament and the Council for electronic identification and trust services for electronic transactions in the domestic market" are analyzed. The conclusion of the relevance and the need of Ukraine's accession to the electronic digital EU market and related research and development performance are presented. The status of public key infrastructure practice application in European Union and electronic digital signature in Ukraine is analyzed. The basic issues that emerged in the application of electronic digital signature such as unification, standardization, interoperability, scalability, cryptographic stability, complexity of cryptographic transformations are adducted. proposals are developed, and the essence and conditions of the main provisions for the practical implementation of the Regulation, including the future of Ukraine are defined. Requirements that must be addressed in the EU to provide secure electronic services for electronic identification, electronic authentication, electronic signature, electronic seals, electronic time stamps, electronic documents, electronic service delivery and web-site authentication are identified.

Keywords: electronic digital EU market electronic transaction mechanisms for identification, authentication and electronic trust services.

Горбенко Юрій Іванович, кандидат технічних наук, технічний директор АТ "ІІТ".
E-mail: GorbenkoU@iit.kharkov.ua
Горбенко Юрий Иванович, кандидат технических наук, технический директор АО "ИИТ".
Gorbenko Yuriy, Candidate of Technical Sciences, technical director JSC "IIT".