СУТНІСТЬ ЗАКОНОДАВЧИХ ОСНОВ ТА УМОВИ НАДАННЯ ДОВІРЧИХ ПОСЛУГ
В ЄВРОПЕЙСЬКОМУ СОЮЗІ В ПЕРИОД 2015 – 2030 РР.

Юрій Горбенко

Розглядаються питання статусу та необхідності удосконалення нормативно – правової законодавчої бази Європейського співвалю (ЄС) відносно електронних довірчих онов на внутрішньому ринку. Аналізуються основні положення "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку". Розбирається вигода про актуальність та необхідність приведення України до електронного цифрового ринку ЄС та проведення відповідних досліджень та виборчих розробок. Аналізується стан впровадження інфраструктури відкритого ключа, а в Україні системи ЕЦП, на практиці. Наводяться основні проблеми питаннями, що виникли в процесі застосування ЕЦП, - уніфікації, стандартизації, електронної, міжнародності, криптографічних та інших аспектів. Розглядається проблема використання відкритого ключа і його внесок до порядку цифрових документів. Висновки подано у вигляді рекомендацій для практичного використання та інших навчальних матеріалів.

Ключові слова: електронний цифровий ринок ЄС, електронні операції, криптографічні сертифікти, відкритий ключ.

Основними проблемами питаннями, які виникли в процесі застосування ЕЦП, є питання ідентифікації, стандартизації, сумісності, масштабування, криптографічної стійкості, складності криптографічних перетворень, а також відповідність значному числу інших вимог [1-3, 6-7]. Їх вирішення здійснювалося на основі міжнародної, національної та регіональної стандартизації алгоритмів ЕЦП, внаслідок чого з'явився значний рівень стандартизації та механізмів [1-2]. В Україні для вирішення значного числа викладених проблем були прийняти законо від 2000 року [5, 6]. Це складними стали питання ідентифікації технічних специфікацій форматів даних [1, 2] тощо, їх реалізації з забезпеченням захисту від компрометації особистих ключів та компрометації засобів криптографічного захищу в цілому.

Внаслідок вказаного знову з'явився деякі національних чи регіональних стандартів, наприклад в ЄС. В той же час визнано, що зміцнення довіри у он-лайн середовищі є ключом до економічного розвитку [11]. Відсутність довіри змушує споживачів, бізнес і керівництво коливатися при змінних операціях в електронному вигляді та приймати нові послуги. Тому в ЄС визнано ряд існуючих обмежень відносно електронного (цифрового) розвитку Європи і запропоновано нові та законодавство про електронні підписи, взаємне визнання електронної ідентифікації та електронної автентифікації, а також необхідність розроблення та прийняття чітких законодавчих основ, забезпечення сумісності, підвищення використання громадянами електронних систем та суттєвого забезпечення кібербезпеки. Необхідність вирішення вказаних задач є необхідною умовою реалізації єдиного електронного ринку, що вже закріплено в Акції про Єдиний Ринок ЄС [11]. Вказано вимагає запровадження в ЄС законодавства, яке забезпечувало б взаємне визнання електронної ідентифікації та автентифікації на всій території ЄС, а також вирішило противіччя, що закладені в положеннях Директив про електронні цифрові підписи [5]. Особливо важливим є взаємне взаємодія та прийняття електронної ідентифікації та автентифікації не зважаючись 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 он-лайн-послуг, електронного бізнесу та електронної торгівлі в ЄС. Дюже 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 й його розширення для забезпечення взаємного визнання та прийняття на рівні ЄС заявних електронних міжнародних ідентифікацій, автентифікацій та інших необхідних електронних довірчих послуг.

Метою цієї статті 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, виявлено певне число протиріч та недоліків. В першу чергу виявлено багато фактів, що недоохоплені до електронних операцій на внутрішньому ринку ЄС. Також визнано, що зміцнення довіри у он-лайн-середовищі є ключом до економічного розвитку, так як відсутність довіри змушує споживачів, бізнес і керівництво обережно відноситись до здійснення операцій в електронному вигляді, особливо...
во приймати нові послуги. Проблемними виводились 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 недостатній рівень кіберзахисності. Вирішення вказаних проблем 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 перегляд положення Директиви про електронні підписи [5] є основоположною дією для реалізації європейського законодавства в 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 чільність електронних операцій між підприємствами, громадянами і державними органами. Законодавство, що є частиною 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, надзійних 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 заявленних електронних схем ідентифікації, електронної автентифікації та інших довірчих послуг (eIDAS).

Аналіз підходів до вирішення вказаних вище завдань показав, що вони базуються на демократичних принципах. Запропонований регламент є результатом широких нарад за участю членів ЄС, в ході цих нарад Комісія зібрала відгуки держав-членів Європейського парламенту та інших зацікавлених сторін. В розробці Регламенту активність проявляли малі та середній бізнес. Детальні матеріали нарад можна знати в [12]. Комісія, що була 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 запровадити прогрівани, що захищені в результаті реалізації Директиви про електронні підписи [5]. Також висловлено думку, що треба ефективніше та оперативніше реагувати на виклики, що винуходять з швидким розвитком нових технологій, зокрема, он-лайн доступу і мобільності доступу, а також зrostання глобалізації.

В результаті роботи комісії були охоплені три набори варіантів політики, що відповідають відпо- відно до сфери: застосування нормативної нової бази; законодавчого інструменту та необхідного рівня контролю. В якості найбільш прийнятного було визначено варіант політики, який спрямований на підвищення правової визначеності, покращення координації з боку національного контролю, забезпечення взаємної визнання та прийняття схем електронної ідентифікації та введення важливих довірчих послуг. Також в ході оцінювання було визначено, що виконання вихідного законодавства може призвести до значного поліпшення правової визначеності, рівня безпеки та довіри до транскордонних електронних операцій. Вказане також призвело до зміщення фрагментації ринку.

2. СУТНІСТЬ ЗАКОНОДАВЧИХ ЕЛЕМЕНТІВ РЕГЛAMENTУ.

Законодавчі елементи Регламенту призначено для усунення існуючих бар'єрів функціонування внутрішнього ринку в ЄС. Вони впроваджені громадянами, підприємствами і державними органами, що отримують користь від взаємного визнання і прийняття електронної ідентифікації, електронної автентифікації, електронних підписів і інших довірчих послуг, не зважаючи на кордони. В ЄС визнано, що Регламент є найбільш підходящим правовим документом. При цьому безпосереднє застосування правил Регламенту визнано законодавчою фрагментацією 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 транснаціональних завдань та рішучих дій, тому що тільки внутрішні, тобто на національній рівні дії самі по собі не є достатньими 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, щоб 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 ж 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 даній час існуючі відмінності в національних законодавствах часто призводять до правової невизначеності і додаткових обмежень. Також правова визначеність з усунення питання значно поліпшиться за рахунок прийняття державами-членами чітких зобов’язань щодо кваліфікованих довірчих послуг. Зазначене створить додаткові стимули для виходу бізнесу за кордон. Так, компанії зможуть брати участь у тендері електронно, що охоплено 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 дбайчи різних правових вимог до довірчих послуг, таких як електронні піломі, електронні документи або відмітки часу. Крім того всі повідомлення про невиконання будуть доставлені з однієї держави-члена до іншої і матимуть юридичну силу в обох державах-членах ЄС. Також торгівля через інтернет буде більш надійною, коли покупці матимуть засіб, щоб переконатися, що вони дійсно зайдуть 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 й дозволять бізнесу вити 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 онлайн податкову декларацію іншій державі-члені ЄС або пацієнту отримати доступ до своїх медичних даних в режимі онлайн. 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 тому вони виходять за майбутнє. Тому в державах здійснюється дублювання робіт, використовуються різні стандарти, а також виникають адміністративні складності при координації шляхом двосторонніх і багатосторонніх уггод. Крім того, існує необхідність вирішення противічів, що пов’язані з відсутністю правової визначеності відносно національних положень, як випливають з різних тлумачень Директив 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 статті.

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

3.1. Електронна ідентифікація.

Статті 5-8 присвячені електронній ідентифікації. В них передбачається взаємне визнання і прийняття засобів електронної ідентифікації, що підпадають під схему (mekanism), яка буде представлена кожного 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 державної 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 буль-яких електронних засобів ідентифікації, що піддають під представлена державою схему на підставі Регламенту визначає існуючі правові бар’єри. При цьому Регламент не зобов’язує держави члени вводити або повідомляти про схеми електронної ідентифікації, але зобов’язує визнавати і приймати представлену електронну ідентифікацію для тих онлайн-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 держави члени повідомляти про свої схеми електронної ідентифікації.

Стаття 6 Регламенту встановлює визначає чотирьоумовні для представлення електронних схем ідентифікації.

1) Держави члени ЄС можуть представляти схеми електронної ідентифікації, які вони прийняли під своєю юрисдикцією для випалювання, коли електронна ідентифікація необхідна для громадських послуг. Іншою вимогою є те, що відповідні електронні засоби ідентифікації повинні бути випущені від імені або прийнятий 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 онлайн автентифікацію для трьох сторін безкоштовно. При цьому автентифікація повинна бути доступна безперервно і ніякі конкретні технічні вимоги, наприклад такі як апаратне або програмне забезпечення, не можуть вважатися сторонами відносно здійснення автентифікації. Але ця вимога не покривається 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 представлена Комісією схем електронної ідентифікації, а стаття 8 вказує на необхідність забезпечення технічної сумісності представленних схем ідентифікації як шляхом координації.

3.2. Довірчі послуги.


Загальні положення. Стаття 9-12 встановлює принципи, що стосуються відповідальності як некваліфікованих, так і кваліфікованих провайдерів довірчих послуг. Вона грунтується на статті 6 Директиви 1999/93/ЄС [6] та поширює право на відшкодування збитків, заподіяних некомпетентним провайдером довірчих послуг. Основною відшкодування збитків слугує доведення нехтування забезпеченням відповідного рівня захисту, що призводить до порушення безпеки. Далі, в статті 10 описується механізм визнання і прийняття кваліфікованих довірчих послуг, наданих провайдером, розташованим в іншій країні. В свою чергу вони грунтується на статті 7 Директиви 1999/93/ЄС, але в регламенті зберегло 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 принципи захисту і мінімізації даних, вони грунтується на статті 8 Директиви 1999/93/ЄС. В ста- тті 12 викладаються особливості надання довірчих послуг інвалідам.

Завдання 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 якнай менше взаємної допомоги між наглядовими органами в державах-членах. Також пропонуються правила спільної діяльності та право участі наглядових органів в такій діяльності. В статті 15 вказується на обов'язки для кваліфікованих і некваліфікованих провайдерів довірчих послуг відповідно технічні та організаційні заходи щодо забезпечення безпеки їх діяльності. Також вимагається щоб у компетентні наглядові органи та інші відповідні органи повинні бути повідомлені 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 викладається вимоги відносно нагляду за кваліфікованими провайдерами довірчих послуг і кваліфікованими довірчими послугами, які надаються ними. Згідно вимог кваліфікованих провайдерів довірчих послуг зобов'язано щорічно проходити перевірку, яка виконується визнаним незалежним органом, щоб надати підтвердження наглядовому органу, що вони виконують свої обов'язки. В статті 17 викладається порядок перевірки та допуску наглядовим органом провайдерів кваліфікованих довірчих послуг до надання ними 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. Вказані інформації про кваліфікованих провайдерів довірчих послуг повинні бути захищені належний рівень деталізації. Нарешті в статті 19 встановлюються вимоги до кваліфікованих провайдерів довірчих послуг, яким вони повинні відповідати, щоб бути визнаними кваліфікованими.
правової визначеності перевірки кваліфікованих електронних підписів викладені обов’язкові вимоги, які грунтується на рекомендаціях Додатку IV Директиви 1999/93/ЄС щодо. У статті 26 викладені вимоги відносно перевірки кваліфікованих послуг електронного підпису, причому кваліфікована послуга перевірки для кваліфікованих електронних підписів повинна надаватись кваліфікованим провайдером довірених послуг. Стаття 27 визначає вимоги відносно довістрокового збереження кваліфікованих електронних підписів. Для цього повинен використовуватись інструменти, механізми і технології, з використанням яких можна продовжувати після зміни часу їх технологічної придатності, термін їхніх змін, але за умови що за цей інтервал змін можуть зробити підробку ключових даних.

Електронні печатки. В статті 28 Регламенту викладені вимоги та умови відносно юридичної сили електронних печаток юридичних осіб. Відносно конкретно правові претензії можуть надаватися лише кваліфікованім електронним печаткам, яка гарантує походження і цілісність електронних документів, що навіть змінени. В статті 29 викладені 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 статті 31 викладені вимоги відносно перевірки та збереження кваліфікованих електронних печаток. Вони грунтуються на статтях 25-27 Регламенту з відповідними змінами щодо юридичної силы електронних підписів.

Електронна цифра часу. Статті 32 Регламенту стосується забезпечення юридичної силі електронних міток часу. При цьому конкретні правові претензії надаються кваліфікованим електронним мітокам 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 силі визнання електронних документів. Також визначаються певні правові претензії автентичності та цілісності будь-якого електронного документа, що зроблені з використанням кваліфікованого електронного підпису або такого, що скрипленого кваліфікованою електронною печаткою. При цьому електронні документи, що видані особами, компетентними відносно видачі відповідних документів і які вважаються оригіналами або їх завіренними копіями відповідно до національного законодавства держави-членки, повинні бути прийняті в іншьих державах-членах без доодаткових вимог.

Послуги електронної доставки. В статті 35 викладаються вимоги відносно юридичної силі даних, що надані або отримані за допомогою послуг електронної доставки. При цьому конкретні правові претензії щодо цілісності даних, які вилізані від отриманні, і точність часу, в якій дані вилізані 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.

Аутентифікація 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 аутентифікації веб-сайту, які можуть бути застосовані для того, щоб гарантувати справжність веб-сайту. При цьому кваліфікований сертифікат аутентифікації веб-сайту повинен надавати мінімальну кількість достовірної інформації про веб-сайт та про легальні існування своєї 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 законодавству делегувати Комісії повноваження приймати не законодавчі акти загального застосування, щоб доповнити або змінити певні несугтєві елементи законодавчого акту.

Що стосується реалізації 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 визначених актів ЄС. Також може застосовуватись процедура експертизи.

3.4 Прикінцеві положення та бюджетні питання.

Присвідчення положення. В параграфах прикінцевих положень викладені питання необхідності, чи необхідно обов’язково Комісії відносно вивчення та аналізу Регламенту. Так згідно статті Комісія визнає, що викладені в даному документі, що визначаються відповідними законодавчими органами.
виносиви. Дуже важливе є те, що в статті 41 вказується про скасування Директиви 1999/93/ЄС і про необхідність забезпечення плавного переходу від існуючої інфраструктури електронного підпису до нових вимог Регламенту. Статтю 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 ВІДНОСИ НО РЕГЛАМЕНТУ ТА ЙОГО ЗАСТОСУВАННЯ В УКРАЇНІ.

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

В ЄС визнають, що зміцнення довіри у онлайн-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. Таким чином Регламент визначено як існування відносно електронного (цифрового) розвитку Європи і запропоновано нові законодавство 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 і інших необхідних електронних довірчих послуг.

5. Основними проблемами питаннями, що виникли в процесі застосування в ЄС ЕЦП, стали питання уніфікації, стандартизації, схематичні, масштабування, класифікації, складності класифікації перетворень тощо. Вирішення вказаних проблемних питань здійснювалося на основі міжнародної, національної та регіональної стандартизації ЕЦП, внаслідок неузгоджених дій в указаному напрямку з'явилось значне число, як правило, несумісних стандартів та механізмів.

6. В зв'язку з цим Регламент Європейського Парламенту та Ради щодо електронної ідентифікації та тараканих сервісів для електронних операцій від 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 операцій між підприємствами, громадянами і державними органами. Його впровадження дозволить підвищити ефективність державних і приватних онлайн-послуг, електронного бізнесу та електронної торгівлі в ЄС.
цій в електронному вигляді, особливо приймати нові посуги. Проблемними виявилися питання, що стосуються електронних підписів, взаємного визнання електронної ідентифікації та електронної автентифікації, наявність необґрунтованої фрагментації та неузгодженності, 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 такового 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 захисту транскордонних та міжрегіональних, надійних і простих електронних операцій, що включають електронну ідентифікацію, автентифікацію та електронні підписи. Метою ухвалення законодавства є покращення існуючого законодавства і його розширення для забезпечення взаємного визнання і прийняття на рівні ЄС заявленних електронних схем ідентифікації, електронної автентифікації та інших довірчих послуг.

9. Аналог підряд до вирішення вказаних протиріч показав, що запропонований Регламент є результатом широкої участі учасників європейської сфер від громадян Європейського парламенту та інших зацікавлених сторін. В розробці Регламенту активність проявив майже всі середній бізнес.

10. Комісія, що була створена в ЄС, також запустила ряд досліджень щодо електронної ідентифікації, автентифікації, електронного підпису та пов’язаних з ним довірчих послуг. При проведенні нарад стало зрозуміли, 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 виникали з швидким розвитком нових технологій, зокрема, онлайн доступу та двобічності доступу, а також зростанням процесів глобалізації.

11. За результатами досліджень в якості найбільш прийнятного визнають орієнтацію, 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 поширення правової визначеності, рівня безпеки та довіри до транскордонних електронних операцій.

12. Основними принципами, що закладені в Регламент ее принципи дотриманості та тестування ефективності. Сутність принципу дотриманості зводиться до розгляду транс національних завдань та їх виконання. Освідчення законодавства, що втрутити внутрішні, тобто на національному рівні дії само 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 виключно на транскордонних аспектах електронної ідентифікації. Розроблений та запропонований Регламент створює рівні умови для підприємств, що надають довірчі послуги.

14. Існуючі відмінності у національних законодавствах часто призводять до правової невизначеності і довіркових обмежень. Таким правовим визначенням з усунення електронних послуг є важливою для використання державами-членами чітких зобов’язань щодо кваліфікації довірчих послуг. Вказане створює дотриманість для вирішення бізнесу за кордон.

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

16. Регламент ЄС не зобов’язує державчото вводити або повідомляти про схеми елект-
розновидної ідентифікації, але зобов'язує визнати і прийняти представлену електронну ідентифікацію для тих, хто вийшов у послугу, де електронна ідентифікація необхідна щоб отримати доступ на національному рівні.


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


20. У випадку інтеграції або асоціації України в ЄС, все що викладене в Регламенті в повній мірі є актуальним і для України. Тим більше, що Україна в сутий 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 перший етапі для торгових відношень з Європою.

21. Наведені в цій статті результати аналізу та дослідження дозволяють зробити висновок та пропозиції відносно необхідності від слідкування та оцінки руху Європейського ринку до електронного, визначення 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 пропаганді напряму улюблення 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 електронній підписі".

**ЛІТЕРАТУРА**

[3]. Директива 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства.
[5]. Закон України „Про електронний документ та електронний документоох” №851-IV від 22.05.2003.
[6]. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" № 2504 – 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 Російської Федерації "Об електронній цифровий підпис" від 10 января 2002 г.

**REFERENCES**

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 банковской системе ЕС и проведения соответствующих исследований и выполнения разработок. Анализируются состояния внедрения инфраструктуры открытою 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 межтак времени, электронных документов, услуг электронной доставки и проверки подлинности веб-сайтов.

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


The problems of the condition and the need to improve the regulatory and legal legislative base of the European Union (EU) for electronic trust services 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 added. 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.