УДК 681.3. 06 (07)

Ю.І. ГОРБЕНКО, канд. техн. наук

СУТНІСТЬ ТА НЕОБХІДНІСТЬ ВИКОНАННЯ ДОДАТКОВИХ ВИМОГ ВІДНОСНО НАДАННЯ ДОВІРЧИХ ПОСЛУГ В ЄС ТА УКРАЇНІ В ПЕРІОД 2015 – 2030 рр.

Вступ

В Європейському Союзі (ЄС) визнано, що зміцнення довіри у он-лайн-середовищі внутрішнього ринку є ключем до його економічного розвитку. В той же час відсутність довіри змушує споживачів, бізнес і керівництво бути в значній невизначеності при здійсненні операцій в електронному вигляді на внутрішньому ринку ЄС [1, 2]. Але основоположним принципом внутрішнього ринку в ЄС є те, що не повинно бути ніяких обмежень на надання довірчих послуг провайдерами довірчих послуг на території держави-члена, розташованими в інших державах-членах [2]. У зв'язку з необхідністю вирішення в ЄС вказаних протиріч прийнято суттєво значущий документ – "Регламенту Європейського Парламенту та Ради щодо електронної ідентифікації та трастових сервісів для електронних операцій на внутрішньому ринку" – в подальшому Регламент [3]. Він призначений забезпечити безпечні і цілісні електронні операції між підприємствами, громадянами і державними органами, що дозволить підвищувати в ЄС ефективність державних і приватних онлайн – послуг у різних сферах. Регламент є основоположним перспективним нормативно – правовим документом, який розроблений на основі значного досвіду створення, застосування, та розвитку інфраструктури відкритого ключа в ЄС, основним його призначенням є забезпечення безпечних, цілісних електронних довірчих операції в ЄС.

Нині розпочато аналіз основних положень, вимог та, саме основне, розробки чи визначення принципів, механізмів та методів реалізації Регламенту в ЄС. Але при аналізі та дослідженнях в значній мірі випущені проблемні питання, особливості , вимоги та механізми реалізації положень Регламенту, що викладені в його додатках [3]. Вони, на наш погляд, стосуються усіх безпечних електронних послуг щодо електронного підпису, електронних печаток, електронних міток часу, електронних документів, послуг електронної доставки та перевірки справжності веб-сайту [3].

Мета статті – аналіз сутності, особливостей, вимог та механізмів реалізації положень Регламенту, що викладені в додатках до нього, а також визначення задач щодо їх врахування чи виконання при надання безпечних електронних послуг щодо електронного підпису, електронної печатки, електронних документів, послуг електронної доставки та перевірки справжності веб-сайту.

Досягнення цієї мети дозволить визначити та реалізувати більш коректно вимоги Регламенту, зважаючи на необхідність використання існуючої системи цифрового підпису.

В додатках I, II, III та IV Регламенту [3] наведено вимоги до кваліфікованих сертифікатів електронного підпису, пристроїв створення кваліфікованого підпису, кваліфікованих сертифікатів електронних печаток та кваліфікованих сертифікатів автентифікації веб-сайту. Вони в суттєвій мірі засновані на діючій Директиві [4]. Розглянемо їх та проведемо аналіз у відповідності з метою, що викладена вище.

1. Основні визначення відносно кваліфікованих сертифікатів електронного підпису

Спочатку, для однозначного тлумачення, розглянемо основні поняття та визначення, що стосуються вдосконаленого та кваліфікованого електронного підпису, а також засобів і особливостей їх реалізації [3].

"Підписувач" – це фізична особа, яка створює електронний підпис.

"Електронний підпис" – це дані в електронній формі, які приєднуються або логічно пов'язуються з іншими електронними даними, і використовуються підписувачем в якості підпису.

"Вдосконалений електронний підпис" – це електронний підпис, що відповідає вимогам а) – г), що наведені нижче:

а) електронний підпис однозначно пов'язаний з підписувачем;

б) електронний підпис може ідентифікувати підписувача;

в) електронний підпис виробляється з використанням даних його вироблення, які підписувач може, з високим ступенем впевненості, одноосібно контролювати;

г) електронний підпис пов'язаний з даними, до яких він відноситься, таким чином, що будь-яка наступна зміна даних може бути виявлена.

"Кваліфікований електронний підпис" – це вдосконалений електронний підпис, який створюється пристроєм для створення кваліфікованого електронного підпису, і базується на кваліфікованому сертифікаті для електронних підписів.

"Дані вироблення електронного підпису" – це унікальні дані, які використовуються підписувачем для створення електронного підпису.

"Сертифікат" – це електронний атестат, що пов'язує дані для перевірки електронного підпису або печатки фізичної чи юридичної особи, з відповідним сертифікатом і підтверджує ці дані.

"Кваліфікований сертифікат електронного підпису" – це атестат, який використовується для підтримки електронних підписів, видається провайдером кваліфікованих довірчих послуг і відповідає вимогам, викладеним у Додатку I [4].

Визначення в частині довірчих послуг.

" Пристрої для створення електронного підпису" – налаштоване програмне або апаратне забезпечення для створення електронного підпису;

"Пристрій для створення кваліфікованого електронного підпису" – пристрій для створення електронного підпису, що відповідає вимогам, викладеним у Додатку II регламенту [4].

2. Сутність та аналіз вимог до кваліфікованих сертифікатів електронного підпису

Згідно вимог додатку I [3] кваліфіковані сертифікати електронного підпису повинні містити:

а) вказівку, принаймні у формі, придатній для автоматизованої обробки, що сертифікат був виданий в якості кваліфікованого сертифіката електронного підпису;

б) набір даних, які однозначно визначають провайдера кваліфікованих довірчих послуг, що видав кваліфіковані сертифікати, і містить, принаймні, найменування держави-члена, в якій провайдер розташований, а також такі дані :

– для юридичної особи: найменування та реєстраційний номер, які наводяться в офіційних документах;

– для фізичної особи: ім'я особи;

в) набір даних, що однозначно представляють підписувача, якому видано сертифікат, включаючи, принаймні, ім'я підписувача або псевдонім, що має бути визначений як такий;

г) дані для перевірки електронного підпису, які відповідають даним для створення електронного підпису;

д) відомості про початок і кінець періоду дії сертифікату;

е) ідентифікуючий код сертифікату, що має бути унікальним для даного провайдера кваліфікованих довірчих послуг;

є) вдосконалений електронний підпис або вдосконалену електронну печатку провайдера кваліфікованих довірчих послуг, що видав сертифікат;

ж) місце, де сертифікат вдосконаленого електронного підпису або вдосконаленої електронної печатки, зазначених у пункті є), є доступним безкоштовно;

з) місце розташування послуги перевірки статусу дійсності сертифіката, яка може бути використана для отримання інформації про статус дійсності кваліфікаційного сертифіката;

і) місце де в пристроях створення кваліфікованого електронного підпису знаходяться дані створення електронного підпису, пов'язані з даними перевірки електронного підпису, що належним чином вказано, принаймні у формі, придатній для автоматизованої обробки.

Аналіз показує, що додаткові вимоги до кваліфікованих сертифікатів електронного підпису, що наведені в додатку I [3], висунуті у зв'язку з необхідністю в максимальній мірі врахувати вимоги та практичні результати реалізації Директиви [4]. В системі ЕЦП України перелік та сутність вимог до сертифікатів ЕЦП наведено аналогічні дані [5]. Обидва документи ґрунтуються на діючих стандартах, в Україні на [6], а на міжнародному рівні на [7]. Для електронного підпису в ЄС також необхідно враховувати нормативні документи CEN/ISSS – серію CWA. В цілому додаткові вимоги наведені в достатньо узагальненому вигляді, тому Комісія [1,2], на наш погляд, може регулювати обов'язковість чи необов'язковість певних даних делегованими їй актами [1 -3].

3. Сутність та аналіз вимог до пристроїв створення кваліфікованого підпису

Згідно вимог додатку II[3], до пристроїв створення кваліфікованого підпису висуваються такі вимоги:

1. Пристрої створення кваліфікованого електронного підпису повинні за допомогою відповідних технічних та процедурних засобів гарантувати, що принаймні:

а) забезпечується секретність даних для створення електронного підпису, які використовуються для вироблення електронного підпису;

б) дані для створення електронного підпису, які використовуються для вироблення електронного підпису, можуть бути створені тільки один раз;

в) дані для створення електронного підпису, які використовуються для вироблення електронного підпису, з достатньою впевненістю, не можуть бути отримані, а електронний підпис захищений від підробки шляхом використання наявних в даний час технологій;

г) дані для створення електронного підпису, які використовуються для вироблення електронного підпису, можуть бути надійно захищені законним підписувачем від використання іншими.

2. Пристрої створення кваліфікованого електронного підпису не повинні змінювати дані, що підписуються, або перешкоджати представленню таких даних підписувачу до підписання.

3. Генерація і управління даними для створення електронного підпису повинні виконуватися провайдером кваліфікованих довірчих послуг від імені підписувача.

4. Провайдери кваліфікованих довірчих послуг, що управляють даними для створення електронного підпису від імені підписувача, можуть дублювати дані для створення електронного підпису з метою резервування, якщо виконуються наступні вимоги:

а) безпека дубльованих наборів даних повинна бути на тому ж рівні, що і для оригінальних наборів даних;

б) кількість дубльованих наборів даних не повинна перевищувати мінімальну, що необхідна для забезпечення безперервності обслуговування.

Таким чином додаткові вимоги до пристроїв створення кваліфікованого підпису, що наведені в додатку II [3], висунуті у зв'язку з необхідністю в максимальній мірі врахувати вимоги та практичні результати реалізації Директиви [4] ЄС та враховувати нормативні документи ЄС CEN/ISSS – серію CWA. Додаткові вимоги до пристроїв створення кваліфікованого підпису наведені в дещо узагальненому вигляді, тому Комісія [1, 2] , на наш погляд, може регулювати обов'язковість чи необов'язковість вимог до пристроїв створення кваліфікованого підпису делегованими їй актами [1 – 3], а також здійснювати нагляд за їх виконанням.

4. Сутність та аналіз вимог до кваліфікованих сертифікатів електронних печаток

Згідно вимог додатку III [3], кваліфіковані сертифікати електронних печаток повинні містити такі дані:

а) вказівку, принаймні у формі, придатній для автоматизованої обробки, що сертифікат був виданий в якості кваліфікованого сертифіката електронної печатки;

б) набір даних, які однозначно визначають провайдера кваліфікованих довірчих послуг, що видав кваліфіковані сертифікати, і містить, принаймні, найменування держави-члена, в якій провайдер розташований, та:

- для юридичної особи: найменування та реєстраційний номер, які наводяться в офіційних документах;
- для фізичної особи: ім'я особи;

в) набір даних, що однозначно представляють юридичну особу, якій видано сертифікат, включаючи, принаймні, найменування та реєстраційний номер, які наводяться в офіційних документах;

г) дані для перевірки електронної печатки, які відповідають даним для створення електронної печатки;

д) відомості про початок і кінець періоду дії сертифікату;

е) ідентифікуючий код сертифікату, що має бути унікальним для провайдера кваліфікованих довірчих послуг;

є) вдосконалений електронний підпис або вдосконалену електронну печатку провайдера кваліфікованих довірчих послуг, що видав сертифікат;

ж) місце, де сертифікат вдосконаленого електронного підпису або вдосконаленої електронної печатки, зазначених у пункті (G), є доступним безкоштовно;

з) місце розташування послуги перевірки статусу дійсності сертифіката, яка може бути використана для отримання інформації про статус дійсності кваліфікаційного сертифіката;

і) місце, де в пристроях створення кваліфікованої електронної печатки знаходяться дані створення електронної печатки, пов'язані з даними перевірки електронної печатки, що належним чином вказано, принаймні у формі, придатній для автоматизованої обробки.

В цілому аналіз додаткових вимог до кваліфікованих сертифікатів електронних печаток, що наведені в додатку III [3], висунуті у зв’язку з необхідністю в максимальній мірі врахувати вимоги та практичні результати реалізації електронних печаток , які використовують в діючій системі згідно Директиви [4]. В системі ЕЦП України сертифікати електронних печаток виробляються на основі посилених сертифікатів ЕЦП [9]. Обидва документи ґрунтуються на діючих стандартах, в Україні на [6], а на міжнародному рівні на [7]. Також при застосуванні, в змісті при розробленні електронної печатки, в ЄС необхідно враховувати нормативні документи CEN/ISSS – серію CWA. В цілому додаткові вимоги до кваліфікованих сертифікатів електронних печаток наведені в дещо узагальненому вигляді, тому Комісія [1,2] , на наш погляд, може регулювати обов’язковість вимоги до кваліфікованих сертифікатів електронних печаток делегованими їй актами [1-3].

5. Сутність та аналіз вимог до кваліфікованих сертифікатів автентифікації веб-сайту

Аналіз джерел відносно автентифікації веб-сайтів дозволяє зробити висновок, що ця сфера не достатньо стандартизована та уніфіковано і є новою у самій загальній постановці задачі електронної автентифікації. Тому, на наш погляд в цьому напрямі потрібно ще проводити ряд НД ДКР, результатом виконання яких були б нормативно-правова база, механізми, протоколи, методи та засоби електронної автентифікації веб-сайтів.

Згідно вимог додатку IV[3], кваліфіковані сертифікати автентифікації веб-сайту.

повинні містити:

а) вказівку, принаймні у формі, придатній для автоматизованої обробки, що сертифікат був виданий в якості кваліфікованого сертифіката для автентифікації веб-сайту;

б) набір даних, які однозначно визначають провайдера кваліфікованих довірчих послуг, що видав кваліфіковані сертифікати, і містить, принаймні, найменування держави-члена ЄС, в якій провайдер розташований, також:

– для юридичної особи: найменування та реєстраційний номер, які наводяться в офіційних документах;

– для фізичної особи: ім'я особи;

в) набір даних, що однозначно представляють юридичну особу, якій видано сертифікат, включаючи, принаймні, найменування та реєстраційний номер, які наводяться в офіційних документах;

г) елементи адреси, в тому числі місто і державу юридичної особи, якій видано сертифікат, як це зазначено в офіційних документах;

д) ім'я (імена) домену, який використовує юридична особа, якій видано сертифікат;

є) відомості про початок і кінець періоду дії сертифікату;

е) код ідентифікації сертифікату, що має бути унікальним для провайдера кваліфікованих довірчих послуг;

ж) вдосконалений електронний підпис або вдосконалену електронну печатку провайдера кваліфікованих довірчих послуг, що видав сертифікат;

з) місце, де сертифікат вдосконаленого електронного підпису або вдосконаленої електронної печатки, зазначених у пункті г), є доступним безкоштовно;

і) місце розташування послуги перевірки статусу дійсності сертифіката, яка може бути використана для отримання інформації про статус дійсності кваліфікаційного сертифіката.

Аналіз вимог до кваліфікованих сертифікатів електронної автентифікації веб-сайтів, що наведені в додатку IV [3], показує що вони висунуті у зв’язку з необхідністю створення практично нової технології, механізмів та засобів захисту веб-сайтів. При розробленні системи виготовлення та обслуговування кваліфікованих сертифікатів електронної автентифікації веб-сайтів необхідно враховувати нормативні документи CEN/ISSS – серію CWA. Аналіз стану системи виготовлення та обслуговування кваліфікованих сертифікатів електронної автентифікації веб-сайтів показує що це є достатньо складною задачею, можна сказати проблемою, яка вимагає значних матеріально – технічних та тимчасових ресурсів. Корегування додаткових вимог кваліфікованих сертифікатів електронної автентифікації веб-сайтів, на наш погляд, також може регулюватися Комісією делегованими їй актами [1 -3].

6. Заходи, задачі та необхідні умови впровадження Регламенту при створенні системи надання в ЄС довірчих послуг

Для виконання Регламенту повинні бути заплановані та здійсненими ряд заходів, забезпечені відповідні умови та вирішені основоположні задачі. До них необхідно віднести такі.

6.1. Порядок виконання.

Потрібна відповідна Постанова, що деталізує вимоги з точки зору адміністративних витрат в цілях реалізації запропонованого Регламенту щодо електронної ідентифікації та довірчих послуг для електронних операцій на внутрішньому ринку.

6.2. Необхідні ресурси.

Відповідно до законодавчої процедури і обговорень з метою прийняття Європейським Парламентом і Радою пропонованого Регламенту, Комісії необхідні дванадцять FTE(full time eqvivalents) щоб розробити відповідні делеговані і виконавчі акти для забезпечення доступності організаційних і технічних стандартів, щоб обробити інформацію, передану державами-членами, зокрема, щоб керувати інформацією, пов'язаною з довіреними списками, з метою забезпечення інформованості зацікавлених сторін – зокрема, громадян про переваги використання електронної ідентифікації, автентифікації, підпису і інших довірених послуг, та щоб почати обговорення вказаних питань з метою досягнення взаємодії на глобальному рівні з третіми країнами.

6.3. Тип пропозиції / ініціативи.

Пропозиція / ініціатива, пов'язана з дією, що пере направлена у відповідь на нову дію

6.4. Цілі. Досягнення багаторічної стратегічної цілі Комісії, що досягається цією внаслідок реалізації пропозиції / ініціативи.

6.5. Загальні цілі.

Загальні цілі пропозиції такі ж, як і у загальних політиках ЄС, серед яких Стратегія ЄС–2020. Вона спрямована на забезпечення того, що Європа перетвориться на розумне, стійке та інклюзивне господарство, що забезпечує високий рівень зайнятості, виробництва та соціальної згуртованості.

6.6. Конкретні цілі.

Конкретні цілі та відповідні види діяльності повинні бути направлені на підвищення довіри до загальноєвропейських електронних операцій та забезпечення транскордонного юридичного визнання електронної ідентифікації, автентифікації, підпису і довірчих послуг, а також високого рівня захисту даних і розширення можливостей користувачів на єдиному ринку .

6.7. Відповідні види діяльності (ABM/ABB). Нормативна база для електронного цифрового порядку для Європи.

6.8. Очікувані результати та вплив.

Створення чіткого нормативно-правового середовища для послуг eIAS, яке допомогло б підвищити зручність користувачам, довіру і впевненість у електронному цифровому світі.

6.9. Показники результатів та вплив:

- існування постачальників eIAS, які здійснюють діяльність у декількох державах-членах ЄС;

- до якого пристрої стають інтероперабельними, наприклад, смарт – карти між секторами та країнами;

- використання eIAS всіма категоріями населення;

- ступінь, до якого eIAS використовуються кінцевими користувачами для національних операцій і міжнародних (транскордонних) операцій;

- ступінь узгодженості законодавства щодо eIAS між державами-членами;

- схеми електронної ідентифікації, повідомлені Комісії;

- послуги, що доступні з використанням повідомлених засобів електронної ідентифікації в державному секторі, наприклад, електронний уряд, електронна охорона здоров'я, електронна юстиція, електронні закупівлі;

- послуги, що доступні з використанням повідомлених засобів електронної ідентифікації в приватному секторі, наприклад, онлайн банкінг, електронна комерція, електронна гра на біржі, вхід до веб-сайтів, безпечні Інтернет – послуги тощо.

6.10. Підстави для пропозиції / ініціативи.

Вимоги, що повинні бути виконані в короткостроковій або довгостроковій перспективі. Різні національні реалізації Директиви про електронні підписи, через відмінності в її тлумаченнях державами-членами, призвели до проблем транскордонної взаємодії і, таким чином, до сегментованого простору ЄС і спотворень на внутрішньому ринку. Вказане супроводжується відсутністю довіри і впевненості в електронних системах, що перешкоджає європейським громадянам отримувати вигоду від такої ж послуги в цифровому світі, як і у фізичному світі.

Додаткові переваги участі ЄС. Дія Регламенту на рівні ЄС буде мати явні переваги в порівнянні з дією на рівні держав-членів. Досвід дійсно показав, що національні заходи, окрім того, що є недостатніми для забезпечення можливості транскордонних електронних операцій, але ще й навпаки, створюють перешкоди для загальноєвропейської взаємодії електронних підписів, і в даний час мають такий же ефект для електронної ідентифікації, автентифікації і довірчих послуг.

Уроки, що винесені з аналогічного досвіду в минулому. Регламент ґрунтується на досвіді роботи з Директивою про електронний підпис і проблемах, що виникли у зв'язку з фрагментованою транспозицією і реалізацією цієї Директиви, які завадили їй в досягненні своїх цілей.

Узгодженість і можливість взаємодії з іншими відповідними інструментами. На Директиву про електронні підписи є посилання в ряді інших ініціатив ЄС, які були створені, щоб усунути проблеми сумісності та транскордонного визнання і прийняття, пов'язані з певними типами електронних взаємодій, наприклад, Директива про послуги, Директиви про громадські закупівлі, переглянута Директива ПДВ (електронне виставлення рахунків) або Європейський Громадянський Ініціативний Регламент.

Крім того, Регламент, що пропонується, забезпечить законодавчу базу, сприятливу для широкого прийняти масштабних пілотних проектів , що будуть виконуватись на рівні ЄС для підтримки розвитку сумісних і надійних засобів електронного зв'язку, в тому числі[3]:

- SPOCS, що підтримує реалізацію Директиви про послуги;
- STORK, що підтримує розвиток і використання сумісних eIDs;
- PEPPOL, що підтримує розвиток та використання сумісних рішень щодо електронних закупівель;
- epSOS, що підтримує розвиток та використання сумісних рішень в області електронної охорони здоров'я;
- eCodex, що підтримує розвиток та використання сумісних рішень електронної юстиції.

6.11. Термін дії і фінансові наслідки.

Прийнято пропозицію / ініціативу необмеженого терміну дії.

6.12. Передбачені режими управління.

Централізоване пряме управління організації роботи та керування зі сторони Комісії.

6.13. Правил моніторингу та звітності.

Перше оцінювання буде проведене через чотири роки після набуття чинності прийнятого Регламенту. Положення щодо звіту, за допомогою якого Комісія звітуватиме Європейському Парламенту та Раді щодо його застосування, включені в Регламент. Наступні звіти будуть представлятися кожні чотири роки. Для оцінювання буде застосовуватися випрацювана методологія Комісії. Оцінювання будуть проводитися за допомогою цільових досліджень з питань реалізації правових інструментів, опитувальників для національних органів, експертних обговорень, семінарів, дослідження Євро думок тощо.

6.14. Системи управління і контролю.

Визначені ризики. Для супроводження пропозиції була проведена оцінка впливу Регламенту. Прийнятий новий правовий інструмент передбачає взаємне визнання і прийняття електронної ідентифікації транс кордонно, поліпшить наявне підґрунтя електронного підпису, зміцнюючи національний нагляд за провайдерами довірчих послуг та надасть юридичну силу і визнання відповідним довіреним послугам. Крім того, вводиться використання делегованих та виконавчих актів в якості механізму для забезпечення наряду з технологічними досягненнями, також і гнучкості.

Методи управління, що передбачаються.

Існуючі та запропоновані методи управління, що застосовуються Комісією, будуть покриватись додатковими асигнуваннями.

6.15. Заходи по запобіганню шахрайства та зловживань.

Існуючі заходи запобігання шахрайству, що застосовуються Комісією, будуть покриватись додатковими асигнуваннями. Виконання робіт у відповідності до Регламенту не має наслідків для поточних витрат.

7. Висновки та пропозиції відносно використання додаткових вимог Регламенту

Проведений аналіз додаткових вимог Регламенту дозволяє зробити такі основоположні висновки, оцінки та пропозиції.

7.1. Вимоги, що наведені в додатках I, II, III та IV Регламенту, є додатковими вимогами до кваліфікованих сертифікатів електронного підпису, пристроїв створення кваліфікованого підпису, кваліфікованих сертифікатів електронних печаток та кваліфікованих сертифікатів автентифікації веб-сайту, які в певній мірі засновані на діючій Директиві[4].

7.2. Додаткові вимоги до кваліфікованих сертифікатів електронного підпису, що наведені в додатку I [3], висунуті у зв'язку з необхідністю в максимальній мірі врахувати вимоги та практичні результати реалізації Директиви [4]. В системі ЕЦП України перелік та сутність вимог до сертифікатів ЕЦП наведено в [5]. Обидва документи ґрунтуються на діючих стандартах, в Україні на [6], а на міжнародному рівні на [7]. Додаткові вимоги наведені в достатньо узагальненому вигляді, тому Комісія [1,2] , на наш погляд, може регулювати обов'язковість чи необов'язковість вимог делегованими їй актами [1 -3].

7.3. Додаткові вимоги до кваліфікованих сертифікатів електронних печаток, що наведені в додатку III [3], висунуті у зв'язку з необхідністю в максимальній мірі врахувати вимоги та практичні результати реалізації електронних печаток , які використовують в діючій системі згідно Директиви [4]. В системі ЕЦП України сертифікати електронних печаток виробляються на основі посилених сертифікатів ЕЦП [9]. Документи ґрунтуються на діючих стандартах, в Україні на [6], а на міжнародному рівні на [7]. В цілому Додаткові вимоги до кваліфікованих сертифікатів електронних печаток наведені в дещо узагальненому вигляді, тому Комісія [1,2] , на наш погляд, може також регулювати обов'язковість вимог до кваліфікованих сертифікатів електронних печаток делегованими їй актами [1 -3].

7.4. Аналіз вимог до кваліфікованих сертифікатів електронної автентифікації веб-сайтів додатку IV [3] показав, що вони висунуті у зв'язку з необхідністю створення практично нової технології, механізмів та засобів захисту веб-сайтів. Аналіз стану системи виготовлення та обслуговування кваліфікованих сертифікатів електронної автентифікації веб-сайтів показує що це є достатньо складною задачею, можна сказати проблемою, яка вимагає значних матеріально – технічних та тимчасових ресурсів. Практичне корегування додаткових вимог кваліфікованих сертифікатів електронної автентифікації веб-сайтів, на наш погляд, в подальшому може регулюватися Комісією делегованими їй актами [1 -3].

7.5. При розробленні системи виготовлення та обслуговування кваліфікованих сертифікатів електронного підпису, кваліфікованих сертифікатів електронних печаток та кваліфікованих сертифікатів електронної автентифікації веб-сайтів, необхідно враховувати нормативні документи CEN/ISSS – серію CWA.

7.6. Загальні цілі Регламенту такі ж, як і у загальних політик ЄС, в яких фігурує дана пропозиція відносно [3], вони визначені в Стратегія ЄС -2020. В цілому вона спрямована на забезпечення того, що Європа перетвориться на розумне, стійке та інклюзивне господарство, що забезпечує високий рівень зайнятості, виробництва та соціальної згуртованості, перше за все за рахунок створення транскордонного електронного світу.

Список літератури: 1. *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). 2. http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision. 3. *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}. 4. *Директива* 1999/93/ЄС Європейського парламенту та Ради від 13 грудня 1999 року про систему електронних підписів, що застосовується в межах Співтовариства. 5. *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). 6. *ДСТУ I*TU-T Rec.X.509 | ISO/IEC 9594-8:2006 « Інформаційні технології. Взаємозв'язок відкритих систем. Каталог: Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів». 7. *ISO/IEC* 9594-8:2012.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 05.02.2014