

ДОВІРА ТА БЕЗПЕКА В ЦИФРОВІЙ ЕКОНОМІЦІ

(сфери електронної ідентифікація та електронних довірчих послуг, що охоплюють електронні підписи, печатки, штампи часу, послуги електронної доставки та автентифікацію веб-сайтів, а також сфера безпеки Інтернету, приватних мереж та інформаційних систем, призначених для функціонування суспільства та економіки).

Інформаційно-аналітичний огляд

2018 рік

Зміст

Вступ	2
1. Політика ЄС та ініціатива СхП щодо довіри та безпеки в цифровій економіці	2
2. Національна політика та стан розвитку сфери довіри та безпеки в цифровій економіці	4
3. Досягнення і виклики	4
4. Варіанти політики у сфері довіри та безпеки в цифровій економіці	5

Інформаційно-аналітичний огляд підготовлено експертами проекту [«Посилення участі громадськості у створенні та імплементації цифрового порядку денного України та гармонізації цифрових ринків з ЄС та країнами СхП»](#), який виконує ГС «Центр розвитку інновацій» під егідою Української сторони Платформи громадянського суспільства Україна-ЄС та Української національної платформи Форуму громадянського суспільства Східного партнерства за сприяння Європейського Союзу та Міжнародного фонду «Відродження» в межах грантового компоненту проекту «Громадська синергія».

Вступ

В Україні в інформаційних системах органів виконавчої влади та місцевого самоврядування використовуються різноманітні засоби та механізми електронної ідентифікації користувачів, які недостатньо враховують такі базові принципи, як безпека, захист персональних даних, достовірність ідентифікації, інтероперабельність та зручність використання.

Актуалізація в останній час публічної риторики та розроблення відповідних проектів нормативно-правових актів щодо доцільності використання електронного цифрового підпису при функціонування інформаційних систем для надання і споживання тих чи інших послуг в електронному вигляді, в тому числі адміністративних, а також необхідність виконання взятих Україною зобов'язань в рамках Угоди про асоціацію з ЄС в частині нормативно-правового наближення між Сторонами у секторі телекомунікаційних послуг (додаток 17 до Угоди про Асоціацію з ЄС), доводять необхідність більш глибокого аналізу існуючого законодавства та розробленого на виконання взятих зобов'язань Закону України «Про електронні довірчі послуги».

Постійні технічні зміни, що відбуваються в секторі ІКТ, виводять назовні ланцюг проблем, які не можуть бути вирішені в рамках законів про електрозв'язок або традиційних законів про захист прав споживачів. В європейських країнах ці питання вирішуються шляхом прийняття нових законів та нормативних актів, спеціально орієнтованих на питання, що стосуються захисту прав споживачів в секторі ІКТ, такі як захист прав інтелектуальної власності, захист від спаму, захист конфіденційного характеру інформації (в тому числі персональних даних), захист від шахрайства, кіберзлочинності, а також заходи для електронної торгівлі. Такі законодавчі акти необхідні для створення клімату довіри та впевненості при використанні цифрових мереж.

Забезпечення електронної безпеки є серйозним завданням. І говорячи про «безпеку» різні стейкхолдери застосовували цей термін по-різному - як до окремих осіб, так і до держави, і тому потребуватиме балансу між цими двома системами інтересів.

Запровадження довірчих послуг здійснюватиметься у всіх сферах економіки та функціонування суспільства. Питання довіри до сервісів, ідентифікації користувачів у цифровому світі та безпеки в мережі Інтернет – це виклик для державно-приватного партнерства, оскільки більшість операторів чи провайдерів сервісів знаходяться у приватному секторі економіки.

1. Політика ЄС та ініціатива СхП щодо довіри та безпеки в цифровій економіці

У 2015 році Європейська комісія ініціювала амбіційну стратегію досягнення DSM. Ключовим фактором успіху для отримання повної вигоди DSM є високо конкурентна цифрова індустрія в Європі та інтеграція цифрових інновацій у всі сектори. Застосування цифрових технологій допоможе компаніям вирости за межі внутрішнього ринку ЄС і зробити ЄС ще більш привабливим місцем для глобальних інвестицій. Основна увага приділяється діям з чіткою побудовою європейської вартості, що доповнює і забезпечує розширення національних ініціатив. Вона заснована на залученні усіх відповідних зацікавлених сторін, а саме великих, середніх та малих компаній з усіх галузей промисловості, цифрової галузі постачання, соціальних партнерів, держав-членів та регіонів.

Це супроводжується додатковими документами щодо:

Європейської ініціативи у сфері хмар представлений план створення інфраструктури даних світового класу для науки та техніки, яка забезпечить вчених та інженерів в ЄС широкі можливості для обчислень та обробки даних. Це забезпечить віртуальне середовище з відкритими та

безперебійними службами для зберігання, управління, аналізу та повторного використання досліджень через кордони та дисципліни;

"Пріоритети стандартизації ІКТ" визначає основні стандарти ІКТ та пропонує заходи для прискорення їх розвитку для підтримки цифрових інновацій у всій економіці. Вона визначає пріоритети для стандартів на основі широких консультацій та пропонує конкретні заходи для їх досягнення;

План дій Електронного уряду щодо цифрової трансформації державних послуг зосереджується на потребах бізнесу та громадян, тобто в Інтернеті, транскордонних, взаємодіючих за замовчуванням та рішеннях, які за проектом є кінцевими;

Документ щодо працівників в Інтернеті речей висвітлює виклики та можливості ІТ в Європі.

У Європейському Союзі під "мережевою та інформаційною безпекою" розуміють здатність мережі чи інформаційної системи протистояти певному випадку конфліктності випадкових подій або незаконних або зловмисних дій, що ускладнюють доступність, автентичність, цілісність та конфіденційність збережених або переданих даних та відповідних послуг, пропонує або доступних через ці мережі та системи [30].

Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) створене спеціально для забезпечення взаємодії країн ЄС у досягненні безпеки.

Стратегії мережевої та інформаційної безпеки, оприлюднені інституцією, органом, офісом або агентством Союзу або державою-членом, повинні бути надані ENISA для отримання інформації та для уникнення дублювання зусиль. ENISA має аналізувати стратегії, сприяти їх поданню у форматі, що полегшує порівняльність, а також зробити стратегії та їх аналіз доступним для громадськості за допомогою електронних засобів.

Директива з безпеки мережевих та інформаційних систем (Директива NIS) є першою частиною законодавства ЄС щодо кібербезпеки. Директива забезпечує правові заходи для підвищення загального рівня кібербезпеки в ЄС. Вона була прийнята Європейським парламентом 6 липня 2016 року і вступила в силу в серпні 2016 роки, але держави -члени мають 21 місяців, щоб транспонувати Директиву в свої національні закони і більше 6 місяців, щоб визначити операторів основних послуг.

Директива NIS передбачає юридичні заходи для підвищення загального рівня кібербезпеки в ЄС шляхом забезпечення:

- готовності держав-членів, вимагаючи, щоб вони були належним чином обладнані, наприклад, через групу з реагування на інциденти в галузі комп'ютерної безпеки (CSIRT) та компетентний національний орган НІС,
- співробітництва між усіма державами-членами шляхом створення групи співпраці з метою підтримки та сприяння стратегічній співпраці та обміну інформацією між державами-членами. Крім того, їм необхідно буде встановити мережу CSIRT, щоб сприяти швидкому та ефективному оперативному співробітництву щодо конкретних випадків кібербезпеки та обміну інформацією про ризики,
- культури безпеки між секторами, які є життєво важливими для економіки та суспільства, і, крім того, сильно покладаються на ІКТ, такі як енергетика, транспорт, вода, банківська справа, інфраструктура фінансового ринку, охорона здоров'я та цифрова інфраструктура. Підприємства в цих секторах, які визначаються державами-членами як оператори основних служб, повинні будуть вживати відповідних заходів безпеки та повідомляти відповідні національні органи про серйозні інциденти. Крім того, основні цифрові постачальники послуг (пошукові системи, служби хмарних обчислень та інтернет-магазини) повинні відповідати вимогам безпеки та повідомлення відповідно до нової Директиви.

Сьомий пріоритет Східного партнерства - до 2020 року «Зосередження уваги на ключових пріоритетах та відчутних результатах» також підтверджує необхідність узгодження Стратегій щодо безпеки для досягнення єдиного цифрового ринку як в ЄС, так і з третіми країнами.

2. Національна політика та стан розвитку сфери довіри та безпеки в цифровій економіці

Закони України «Про електронний цифровий підпис» та «Про електронні документи й електронний документообіг» встановлюють основні організаційно-правові засади електронного документообігу та використання електронних документів із електронним цифровим підписом (ЕЦП), але ці закони мають бути також оновлені відповідно до Угоди з ЄС в частині переходу від ЕЦП та електронного документа до повноцінного регулювання довірчих е-послуг.

Зазначеним законом передбачено, що договори, укладені в електронній формі, прирівнюються до договорів, укладених у письмовій формі. Електронний договір підписують за допомогою електронного підпису, ЕЦП, електронного підпису з одноразовим ідентифікатором або аналогом власноручного підпису. Проте процедура підписання зазначеним законом не охоплена. Опис процедур допоміг би уникнути ризиків визнання е-договору недійсним. Відсутність належного нормативного регулювання порядку використання електронного підпису чи ЕЦП несе потенційні ризики для сторін угод, укладених у режимі реального часу.

Сферу безпеки регулює Закон України «Про основні засади забезпечення кібербезпеки України» (набирає чинності), Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України",

Яскравим прикладом згуртованої активності та спільних дій стали події, що щодо опрацювання представниками експертного кола у рамках профільного комітету Парламенту, законодавства у сфері електронних довірчих послуг – законодавства, що має на меті розв'язання поставлених РКІ Форум UA (проводиться з 2012 року, учасники – профільні організації та органи влади) завдань. Експертне коло об'єднало багато різнопрофільних фахівців – юристів, спеціалістів з криптографії, представників усіх зацікавлених у запровадженні електронних послуг державних органів, бізнес спільноти, математиків, інші технічні спеціалістів з захисту інформації. Спільна робота тривала у парламентському профільному комітеті тривала майже два місяці.

3. Досягнення і виклики

Роботу над законопроектом щодо електронних довірчих послуг було розпочато у 2012 році фахівцями Міністерства юстиції, членами ГО «ВАІБІТ», експертами та іншими зацікавленими сторонами, до першого голосування у Парламенті щодо цього законопроекту знадобилось майже 5 років. Тепер Закону України «Про електронні довірчі послуги» ще набирає чинності та готується нормативна база щодо його імплементації.

І знову це лише перша сходинка, важливо зараз для усіх зацікавлених сторін не залишатися осторонь та продовжувати спільну роботу вже над подальшою імплементацією норм закону про довірчі послуги після його прийняття, на черзі щонайменше 25 нормативних актів, і ще більший перелік стандартів у рамках діючих різних експертних груп та ТК.

За результатами дискусії учасники РКІ Форум UA 2017 визначили, що важливим напрямом, який потребує розвитку та уваги всіх учасників, **це сфера захисту персональних даних**. Контроль за рухом власних персональних даних пов'язаних з розвитком електронної комерції та розповсюдженням та популяризацією послуг у тому числі, що надаються державою в електронному виді.

Ризик неконтрольованого поширення персональних даних пов'язаний зі зростаючим числом грубих порушень інформаційної безпеки – кібершахрайства, що зростають у такій самій прогресії як і рівень електронної комерції.

Запровадження будь-яких електронних документообігів опиняється у руках установи, яка на підставі документу, затвердженого Мін'юстом, вимагає паперових примірників електронних документів. Також не вирішеним є питання щодо перевірки електронного цифрового підпису на момент передачі на зберігання архівних електронних документів – нормативний документ не визначає порядок перевірки чи зняття підпису у момент передачі архіву разом з програмними комплексами чи окремо.

У разі, якщо не буде розроблено дієвих механізмів управління передачею на зберігання архівних електронних документів, задеклароване швидке переведення державних установ на електронний документообіг, може залишитись тільки декларацією.

Таким чином, потребує вирішення у найближчий час:

- 1) Забезпечення ЦДЕА України достатніми коштами для забезпечення зберігання великих масивів даних (або на колокейшн, або на побудову власних потужностей для зберігання);
- 2) Виділення достатніх людських ресурсів – три відділи ЦДЕА України є недостатньо для побудови великих архівних цифрових фондів;
- 3) Перегляд нормативно-правового забезпечення регулювання питання архівування електронних документів шляхом виключення можливостей повернення до паперових форм документів.

4. Варіанти політики у сфері довіри та безпеки в цифровій економіці

1. Нічого не робити.
2. Розробити нормативні акти на реалізацію Законів України «Про електронні довірчі послуги» та «Про основні засади забезпечення кібербезпеки України», а саме:
 - закласти засади нормативного та технологічного регулювання для сфери електронної ідентифікації та створити умови легалізації нових технологій;
 - кваліфікованим довірчим послугам та електронній ідентифікації стати основою для подальшої розбудови орієнтованої на користувача та безпечної екосистеми електронного урядування, електронної комерції та електронної демократії;
 - вирішити питання транскордонного визнання цифрових підписів для українських громадян та бізнесу та їх європейських партнерів;
 - надати можливість громадянам України використовувати такі засоби ідентифікації, як ID-картка, отримувати публічні послуги в електронній формі не тільки в Україні, але й на території Євросоюзу;
 - зберегти діючу інфраструктуру відкритих ключів в Україні, як одну із найбезпечніших на європейському просторі;

- у відповідності до положень Регламенту створити умови рівноправного функціонування сфери надання довірчих послуг для внутрішнього ринку та потреб безпеки та транскордонної взаємодії;
- підтримати державний сектор надавачів електронних довірчих послуг, які на сьогодні функціонують у сферах юстиції, національної безпеки, залізничного транспорту тощо незалежно від ринкових коливань та тенденцій;
- максимально за змістом та використаними моделями державного регулювання наблизити до європейських процедури доступу до надання послуг, нагляду за їх виконанням;
- переглянути та узгодити переліки та зміст електронних довірчих послуг;
- визначити етапи поступового переходу до визначеної в Регламенті моделі, з урахуванням того, що органи, відповідальні за формування і реалізацію політики у сфері електронної ідентифікації повинні будуть розробити певний перелік підзаконних нормативно-правових актів;
- розробити механізми доступу та можливість використовувати довірчі послуги інвалідами – зобов'язання по Конвенції Організації Об'єднаних Націй про права інвалідів;
- законодавчо чітко визначити необхідність електронного цифрового підпису як складової електронного документу при реалізації електронного урядування та електронної демократії, для електронної комерції – за бажанням;
- розробити законодавчі засади для можливості електронної взаємодії при застосуванні усіх моделей електронного урядування (G2G, G2B, G2C, G2E, G2I).

3. Для залучення всіх зацікавлених сторін і забезпечення комплексного захисту для кібербезпеки пропонуємо розробити узгоджений з європейськими партнерами та усіма зацікавленими сторонами новий план реалізації стратегії кібербезпеки, де буде відображено спільну відповідальність держави та приватних структур, відповідальних за певні напрями кібербезпеки з урахуванням інформації, викладеної у звіті про виконання плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України.

Такий план повинен зачіпати багато різних областей, включаючи висвітлення значення ІКТ для країни; визначення та аналіз ризиків від кіберзлочинності і кібератак; визначення строків, відповідальних за виконання завдань, таких як запобігання і виявлення кіберзлочинів і кримінальне переслідування за такі злочини, розвиток цифрових навичок населення, заходи розвитку «цифрової гігієни» тощо.

Заслухавши та обговоривши коло питань, передбачених програмою РКІ Форум UA 2017 (організатор ГО «ВАІБІТ»), який є майданчиком для дискусій стейкхолдерів даного напрямку з 2012 року, учасники вирішили ініціювати звернення щодо:

нормативного урегулювання питань щодо захисту прав споживачів в секторі ІКТ, такі як захист прав інтелектуальної власності, захист від спаму, захист конфіденційного характеру інформації (в тому числі персональних даних), захист від шахрайства, кіберзлочинності, а також заходи для електронної торгівлі;

удосконалення законодавства у сфері захисту персональних даних з метою імплементації актів ЄС у цій сфері та розробки актів технічного регулювання з цих питань;

розробки узгодженого з європейськими партнерами та усіма зацікавленими сторонами нового плану реалізації стратегії кібербезпеки, який буде враховувати необхідність запровадження спільної відповідальності держави та приватних структур в частині управління об'єктами критичної інфраструктури.

Досягнення єдиного цифрового ринку (DSM) з Європейським Союзом та країнами Східного партнерства є необхідною умовою для залучення інвестицій у цифрові інновації та для швидшого зростання бізнесу у цифровій економіці.

1. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства, звіт в рамках проекту «Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз», за загальною редакцією В.Мартинюка (керівника проекту) URL: <http://geostrategy.org.ua>
2. Електронне урядування : навч. посіб. / Семенченко А. І. [та ін.] ; [за ред. А. І. Семенченка] ; Кабінет Міністрів України, Нац. ун-т біоресурсів і природокористування України, Навч.-наук. ін-т післядиплом. освіти. - Херсон : Гринь Д. С., 2014. - 391 с.
3. Інфраструктура відкритих ключів: технології, архітектура, побудова та впровадження : навчальний посібник / Потій О. В., Лешшин А. В., Сорока Л. С., Єсін В. І., Мороз Б. І. - Дніпропетровськ : Академія митної служби України, 2011. - 202с.
4. Деякі питання удосконалення системи ідентифікації особи і функціонування державних та єдиних реєстрів Розпорядження Кабінету Міністрів України URL: <http://zakon2.rada.gov.ua/laws/show/628-2015-%D1%80>
5. Олексюк Л. В. Механізми правового забезпечення електронного доступу до публічної інформації та відкритих даних: стан та тенденції розвитку. Держ. упр. та місцеве самоврядування: зб. наук. пр. Дніпро: ДРІДУ НАДУ, 2016. Вип. 3 (30). С. 92–99.
6. Олексюк Л. Правовые механизмы обеспечения работы с электронными документами. Вест. ун-та Кайнар. (Казахстан) Алматы: Изд-во Академии Кайнар, 2016. № 3. С. 86–91.
7. Олексюк Л. В. Законодавче регулювання ідентифікації фізичних та юридичних осіб в електронних урядуванні, демократії та комерції. Державне управління: удосконалення та розвиток, 2017. № 4. URL: <http://www.dy.nayka.com.ua>.
8. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством [...]Україна, Європейський Союз, Євратом; Угода, Міжнародний документ від 27.06.2014 URL: http://zakon4.rada.gov.ua/laws/show/984_a11
9. COMMISSION DELEGATED REGULATION (EU) supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (2017), by the European Commission URL: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/amending-and-supplementary-acts/implementing-and-delegated-acts_en
10. Selected articles on Authentication (2014-18), by Heather Walker, Luis Balbas, Guillaume Forget, Jan Kjaersgaard, Dawn M. Turner and more URL: <https://www.cryptomathic.com/news-events/blog/topic/authentication>
11. Selected articles on Electronic Signing and Digital Signatures (2014-todays), by Ashiq JA, Guillaume Forget, Jan Kjaersgaard, Peter Landrock, Torben Pedersen, Dawn M. Turner, Tricia Wittig and more URL: <https://www.cryptomathic.com/news-events/blog/topic/authentication>
12. The European Interoperability Framework - Implementation Strategy (2017), by the European Commission URL: http://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_1&format=PDF
13. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (2016), by the European Commission
14. REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016), by the European Parliament and the European Council

15. Proposal for a REGULATION concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), (2017), by the European Parliament and the European Council
16. Revised Directive 2015/2366 on Payment Services (commonly known as PSD2) (2015), by the European Parliament and the Council of the European Union
17. REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014) by the European Parliament and the European Commission
18. DIRECTIVE 2013/37/EU amending Directive 2003/98/EC on the re-use of public sector information (2013) by the European Parliament and the Council
19. Recommendations for the Security of Internet Payments (Final Version) (2013), by the European Central Bank
20. Draft NIST Special Publication 800-63-3: Digital Authentication Guideline (2016), by the National Institute of Standards and Technology, USA.
21. NIST Special Publication 800-63-2: Electronic Authentication Guideline (2013), by the National Institute of Standards and Technology, USA.
22. Security Controls Related to Internat Banking Services (2016), Hong Kong Monetary Authority
23. Digital Single Market Policies about Open Internet & Net neutrality <https://ec.europa.eu/digital-single-market/en/policies/76013/3581>
24. BENEDIKT LUFT Connectivity Six Cyber Threats to Really Worry About in 2018 https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/?utm_campaign=add_this&utm_source=twitter&utm_medium=post
25. ЗВІТ ПРО ВИКОНАННЯ УГОДИ ПРО АСОЦІАЦІЮ МІЖ УКРАЇНОЮ ТА ЄВРОПЕЙСЬКИМ СОЮЗОМ У 2017 РОЦІ https://www.eu-ua.org/sites/default/files/imce/layout_16_02_final.pdf
26. Директива 2000/31/ЄС Європейського парламенту та Ради «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку» URL: http://zakon1.rada.gov.ua/laws/show/994_224
27. Директива № 2002/58/ЄС Європейського парламенту та Ради стосовно обробки персональних даних та захисту конфіденційності в секторі електронних засобів зв'язку URL: http://zakon1.rada.gov.ua/laws/show/994_b34/print1391002515982815
28. Про захист персональних даних Верховна Рада України; Закон України Закон від 01.06.2010 № 2297-VI URL: <http://zakon3.rada.gov.ua/laws/show/2297-17>
29. Порядок роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання URL: http://tsdea.archives.gov.ua/ua/?page=1886_11112014
30. Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0526>
31. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
32. Eastern Partnership – 20 Deliverables for 2020: focusing on key priorities and tangible results URL: https://eeas.europa.eu/sites/eeas/files/20_deliverables_for_2020.pdf