

# Передумови Інтеграції України до Єдиного Цифрового Ринку ЄС

Гречко А.В.

Інститут кібернетики ім. В.М. Глушкова НАНУ,  
відділ автоматизації програмування  
Україна, Київ, пр. Глушкова, 40,  
grechna@gmail.com

., Мелашенко А.О.

Інститут кібернетики ім. В.М. Глушкова НАНУ,  
відділ автоматизації програмування  
Україна, Київ, пр. Глушкова, 40,  
javatask@gmail.com

**Анотація** – В роботі описані ключові етапи інтеграції України до єдиного цифрового ринку ЄС. Викладений поточний стан сфери електронної ідентифікації та довірчих послуг, а також надані рекомендації із прищвидження розбудови базової цифрової інфраструктури.

**Ключові слова:** Будівельний блок CEF, довірчі послуги, електронний документ (ЕД), електронний цифровий підпис, цифровий безвіз.

## I. ВСТУП

Розвиток Інтернету та цифрових технологій поступово перетворює наш світ, у кожній сфері повсякденного життя та у будь-якій галузі бізнесу. У Європейському Союзі вже давно зрозуміли, що необхідно прийняти цифрову революцію та розширити цифрові можливості для людей та підприємств, використовуючи потенціал Єдиного європейського ринку. Європейська Комісія оприлюднила свої докладні плани щодо створення Єдиного цифрового ринку, таким чином реалізуючи один із своїх головних пріоритетів.

Сьогодні бар'єри в Інтернеті означають, що:

- громадяни не мають доступу до багатьох товарів та послуг – лише 15% людей здійснюють покупки в Інтернеті в інших країнах ЄС;
- Інтернет-компанії та стартапи не можуть в повній мірі скористатися можливостями росту в Інтернеті – лише 7% малих та середніх підприємств (МСП) продають свої товари та послуги за кордон [1];
- підприємства та урядові структури недостатньо користуються цифровими інструментами.

Метою Єдиного цифрового ринку є руйнування регуляторних бар'єрів і, врешті решт, перехід від 28 національних ринків до єдиного цифрового ринку ЄС. За деякими оцінками повноцінно функціонуючий Єдиний цифровий ринок може принести до 415 мільярдів євро економії щороку та створити сотні тисяч нових робочих місць.

Прийнята ЄС стратегія Єдиного цифрового ринку включає набір цільових заходів, згрупованих у три категорії:

- кращий доступ для споживачів та підприємств до цифрових товарів та послуг по всій Європі;
- створення належних умов та рівних умов для процвітання цифрових мереж та інноваційних послуг;

- максимізація потенціалу зростання цифрової економіки [2].

Для України це означає, що у відповідності до Угоди про асоціацію та двосторонніх політичних домовленостей вона може “стати членом ЄС” (отримати режим внутрішнього ринку) у сфері електронних комунікацій. Електронних довірчі послуги є частиною сфери електронних комунікацій. Довірчі послуги є предметом цього дослідження. Отже “цифровий безвіз” – це імплементація електронних довірчих послуг між Україною і ЄС, впровадження кодексу електронних комунікацій та директиви з електронної комерції.

Європейський досвід показує, що успішне та ефективне прийняття технологій і створення Єдиного цифрового ринку вимагає спільної роботи і партнерства. Для цього необхідно гармонізувати усі бізнес-, технічні та нормативно-правові аспекти в даній сфері. Хоч з першого погляду це завдання виглядає не дуже складним, на практиці реалізація і підтримка цієї ідеї може зайняти багато років.

Для досягнення потрібного рівня довіри між усіма сторонами в ЄС було прийнято ряд загально визнаних і широко використовуваних правил, зокрема Регламент 910/2014 [3]. eIDAS охоплює електронну ідентифікацію (electronic identification, eID), аутентифікацію (authentication) та довірчі послуги (trust services) і створює основу для гарантування безпечної, швидкої та більш ефективної електронної взаємодії між підприємствами, незалежно від того, в якій країні Європи вони відбуваються. eIDAS є європейським Регламентом, що створює єдину основу для eID та довірчих послуг і робить його більш простим у наданні послуг по всьому Європейському Союзу.

eIDAS сприяє інтероперабельності в усіх 28 країнах-членах ЄС, забезпечуючи в них взаємне визнання через кордони їх схем електронної ідентифікації. Він також гарантує, що довірчі послуги, що надаються постачальниками послуг, які відповідають вимогам Регламенту (наприклад, кваліфіковані постачальники послуг), можуть прийматися в якості доказів в судовому провадженні.

Завдяки eIDAS громадяни, підприємства та органи державної влади можуть використовувати засоби електронної ідентифікації та довірчі послуги (тобто електронні підписи, електронні печатки, штемпелі часу, реєстровану електронну доставку та автентифікацію веб-сайту) для доступу до електронних послуг або управління електронними операціями як у себе в країні так і поза її

межами. Він також створює європейський внутрішній ринок електронних довірчих послуг. Це дозволяє:

- підвищити прозорість та підзвітність – чітко визначено мінімальні зобов'язання та відповідальність для постачальників довірчих послуг (trust service providers, TSP);
- гарантувати надійність послуг разом з підвищенням вимог безпеки для їх провайдерів;
- забезпечити технологічну нейтральність – уникнути вимог, які можна задовольнити лише при використанні певної технології;
- визначити ринкові правила та забезпечити стандартизацію.

Передбачається, що як державні послуги, так і послуги у приватному секторі ставатимуть більш гнучкими і зручними у використанні та запропонують багато інших переваг, включаючи:

- зменшення адміністративного тиску на електронні операції з іншими підприємствами, клієнтами та державними адміністраціями;
- організація більш ефективних бізнес-процесів;
- досягнення економії за рахунок значного скорочення накладних витрат;
- здійснення безпечних електронних транзакцій, що призведе до збільшення довіри споживачів та потенційної споживчої бази – громадяни можуть укласти безпечні транскордонні електронні угоди та повною мірою скористатися своїми правами в ЄС, від зарахування до іноземного університету до доступу до електронних медичних записів;
- зменшення проблем, пов'язаних з безпекою та конфіденційністю, оскільки громадяни та підприємства можуть використовувати свої власні національні електронні ідентифікаційні номери для доступу до електронних послуг;
- збільшення та урізноманітнення державних електронних послуг, що призведе до зменшення обігу паперових документів – громадяни, які переїжджають до іншої держави-члена, можуть реєструватися та користуватися іншими послугами онлайн [4].

Для побудови єдиного цифрового ринку та реалізації норм eIDAS Європейським Союзом було започатковано фонд Програма інтеграції Європи (Connecting Europe Facility, CEF). Він пропонує гранти та іншу фінансову допомогу для підтримки проєктів, які працюють над створенням взаємопов'язаної загальноєвропейської

інфраструктури в енергетиці, транспортній сфері та сфері

цифрових послуг. Ця ключова цифрова інфраструктура широко відома під назвою "будівельні блоки CEF". Вона пропонує основні можливості, які можна використовувати в будь-якому європейському проєкті для полегшення створення міждержавних електронних публічних послуг та розвитку цілих секторів бізнесу.

За своєю суттю будівельний блок CEF – це сукупність технічних специфікацій, програмного забезпечення та послуг, які можна повторно використовувати в проєктах будь-якої сфери діяльності, причому: технічні специфікації будівельного блоку максимально відкриті та орієнтовані на ринок;

послуги будівельного блоку чітко визначені, тобто задокументовані, з угодами про рівень послуг, навчання, забезпечення службою підтримки тощо;

програмне забезпечення будівельного блоку достатньо зріле, тобто пройшло успішне використання в пілотних проєктах для реалізації транскордонних транзакцій.

До переліку основних будівельних блоків зокрема входять:

- електронна ідентифікація eID;
- електронні підписи eSignature;
- електронне виставлення рахунків eInvoicing;
- електронна реєстрована доставка eDelivery;
- електронне архівування eArchiving.

Головна мета CEF – це підтримка проєктів з використання заснованих на стандартах базових компонентів (будівельних блоків), що забезпечуватимуть взаємодію систем між собою. Фонд робить це у такий спосіб:

надає послуги, які допоможуть реалізувати будівельні блоки у будь-якій системі, зокрема послуги з навчання, зразки програмного забезпечення, послуги тестування;

забезпечує грантове фінансування – можна подати заявку на отримання грантового фінансування для оплати впровадження будівельного блоку у будь-якій системі.

На сьогодні будівельні блоки застосовуються у 120 проєктах, таким чином майже 73% галузевої інфраструктури цифрових послуг (Digital Service Infrastructure, DSI) CEF повторно використовують або взяли на себе зобов'язання повторно використовувати принаймні один будівельний блок. Інфографіка щодо повторного використання будівельних блоків у різноманітних галузевих проєктах CEF наведена на рис. 1.

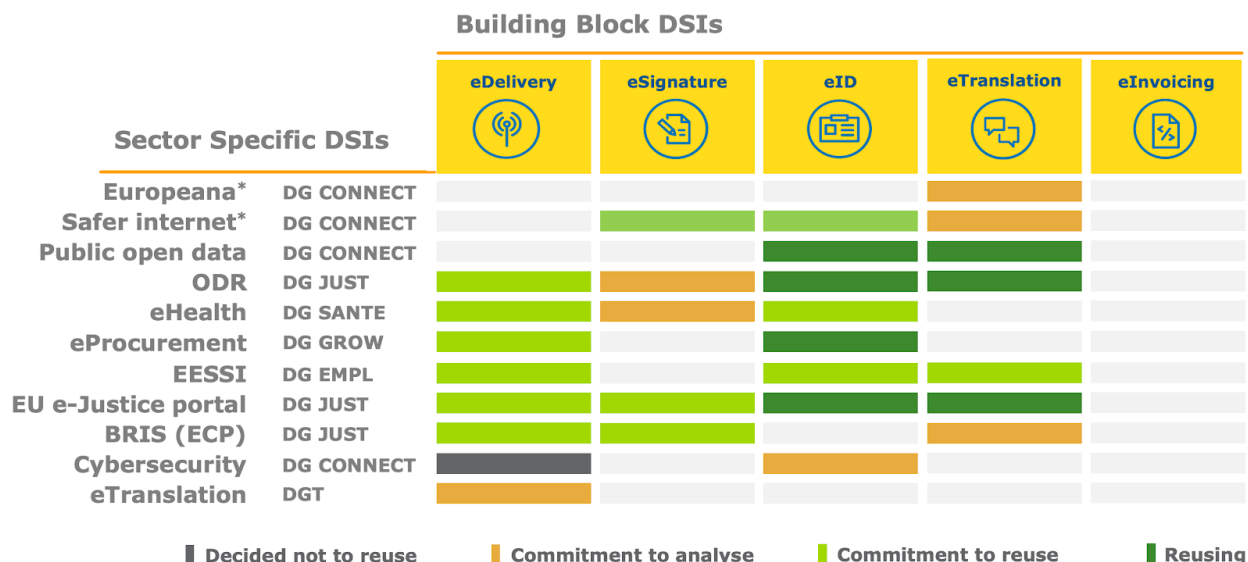


Рис. 1. Розподіл використання будівельних блоків CEF за галузями

## II. ПОВ'ЯЗАНІ РОБОТИ

Дослідження [5] показують, що повторне використання будівельних блоків в якості рішення:

- зменшує витрати завдяки використанню загальних послуг та перевірених технологій;
- скорочує час виходу продукту на ринок – на 40-50% підвищує продуктивність (за такими критеріями ефективності як реальна додана вартість та загальний час виконання);
- просуває спрощеність на всіх рівнях, включаючи підвищену мобільність та розподіл людських ресурсів (обсяг наявних експертних знань), коли рішення на основі будівельних блоків переважають використання систем, “побудованих з нуля”;
- підвищує чутливість до потреб бізнесу та громадян [6].

В якості прикладу реалізації будівельного блоку eSignature можна навести фінансовану ЄС бібліотеку з відкритим вихідним кодом Digital Signature Service (DSS), яку можна використати для реалізації довірчих послуг. Документація до бібліотеки [7] описує деякі приклади розробки на мові Java з використанням фреймворку DSS, що наочно демонструють прогресивний спосіб застосування різноманітних схем та дозволяє розробникам ознайомитись з їх кодом.

В [8] розглянуто досвід успішного впровадження будівельних блоків CEF для побудови інфраструктури цифрових послуг та забезпечення виконання норм Регламенту eIDAS в Естонії.

## III. ОЦІНКА РІВНЯ ЦИФРОВІЗАЦІЇ В УКРАЇНІ

### 3.1 Постановка задачі

Враховуючи досвід Естонії та ті аспекти, що позитивно вплинули на її успіхи на шляху до електронної євроінтеграції, окремо проаналізувати стан:

- нормативно-правової бази;
- технічного забезпечення (використовуваних засобів електронної ідентифікації та існуючих сервісів надання довірчих послуг);
- сфери електронного урядування і електронних послуг в Україні.

Описати перепони, що заважають використовувати будівельні блоки CEF (eSignature та eID) в Україні, та сформулювати рекомендації щодо їх усунення.

### 3.2 Стан нормативно-правової бази у сфері електронної ідентифікації та довірчих послуг в Україні

У розвитку нормативно-правової в нашій країні можна спостерігати досить значні успіхи. У своєму акаунті у Facebook Міністерство цифрової трансформації України навіть оприлюднило деякі результати своєї зустрічі 20 лютого 2020 року з представниками Держспецзв'язку та делегацією EU4Digital – проекту міжнародної технічної допомоги ЄС, що надає підтримку в адаптації українського законодавства до законодавства ЄС. Головний інсайд зустрічі: "Експерти EU4Digital провели попередню оцінку нашого законодавства та технічних вимог і дійшли висновку, що Україна має один з найвищих рівнів імплементації вимог європейського закону про взаємовизнання електронних довірчих послуг eIDAS"<sup>1</sup>. Отже на сьогодні в Україні створена нормативна база з використання ЕЦП при спілкуванні юридичних та фізичних осіб з органами влади:

- розроблений у відповідності до Регламенту 910 та набув чинності у листопаді 2018 року Закон України «Про електронні довірчі послуги», який регулює правові відносини, що виникають між юридичними, фізичними особами, суб'єктами владних повноважень у процесі надання, одержання електронних довірчих послуг;
- прийнято постанову кабінету міністрів України № 992 від 7 листопада 2018 р. «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг», що зробила обов'язковими європейськи

стандарти з довірчих послуг;

- методом підтвердження гармонізовано 120 стандартів ЄС з довірчих послуг.

### *3.3 Стан технічного забезпечення у сфері електронної ідентифікації та довірчих послуг в Україні*

Станом на сьогодні можна зазначити, що технічну можливість використання ЕЦП для ідентифікації в Україні теж вже закладено. Проте наразі ЕЦП масово використовується лише при зверненні в один єдиний орган державної влади – державну фіскальну службу. За підтримки ОБСЄ та Агентства з електронного урядування створені та створюються сервіси надання адміністративних послуг, в яких у цілях верифікації використовується цифровий підпис. Повний перелік діючих в Україні систем, що допускає використання ЕЦП, можна знайти на сайті Інформаційно-довідкового департаменту ДПС.

У деяких регіонах (Одеса, Вінниця) при зверненні громадян до місцевих органів влади використовується e-mail, веб-форма, номер телефону, логін-пароль, соціальні мережі, тощо. Тобто верифікація у цьому випадку не проводиться.

Основними проблемами ЕЦП в Україні є:

- проблеми сумісності, пов'язані з використанням вітчизняних криптоалгоритмів (не визнаних міжнародним співтовариством), несумісні реалізації засобів ЕЦП, обумовлюють вертикальну інтеграцію та наявністю “неконкурентних переваг” певних компаній у певних органах влади, відсутністю чітких стандартів та тестового середовища для інтеграції нових розробок;
- необхідність специфічної сертифікації програмного забезпечення, що гальмує конкуренцію та інновації у цій сфері;
- відсутність авторських прав держави на ЕЦП-інфраструктуру, що у довгостроковій перспективі призводить до більших витрат на закупівлю ліцензій на ПЗ та обумовлюють застосування нестандартизованих рішень певних компаній у певних органах влади.

Оскільки не так багато українців мають ЕЦП, тому в Україні досі залишається проблемою доступність електронних послуг. Покращити ситуацію міг би ID-паспорт (зараз цифровий підпис записується на паспорт нового зразка), проте за даними Державної міграційної служби України з 2016 по 2019 рік включно пластикове посвідчення особи видано лише 4,3 млн. українців, що складає приблизно 10% від всього населення країни (у порівнянні з 98% в Естонії).

Ще однією можливістю отримати унікальний ідентифікатор є запуск в Україні послуги Mobile ID – сервісу, який дозволяє за допомогою мобільного телефону провести ідентифікацію особи для доступу до електронних послуг та використовувати електронно-цифровий підпис в системах електронного документообігу. Для роботи сервісу необхідний звичайний мобільний телефон і спеціальна захищена SIM-карта, яка також має функцію підвищеного захисту інформації.

У 2017 р. мобільний оператор Kyivstar (ПрАТ «Київстар») анонсував запуск у дослідну експлуатацію сервісу Mobile ID, який дозволяє пройти електронну ідентифікацію особи для отримання електронних послуг. Ідентифікація здійснюється шляхом використання мобільного телефону та SIM-картки зі спеціальним чипом. З 2018 р. дана послуга Kyivstar працює в повномасштабному режимі та подається оператором як «цифровий підпис у вашому мобільному», який підходить для використання в електронній комерції, державних установах, охороні здоров'я та інших сферах діяльності. Для користування нею абонент укладає договір про надання послуг Mobile ID, за яким оператор забезпечує генерацію відкритого та особистого ключів, збереження особистого ключа на SIM-карті та використання своєї телекомунікаційної мережі для передачі даних на умовах підключення до спеціального пакету «SMS Mobile ID».

Наприкінці листопада 2018 року аналогічну послугу запровадив й оператор Vodafone Україна (ПрАТ «ВФ Україна»). Останнім у 2019 році запустив вказаний сервіс Mobile ID ще один з найбільших операторів України – Lifecell (ТОВ «Лайфселл»).

З іншого боку, створюються ресурси, за допомогою яких реалізуються інші електронні довірчі послуги. На сьогодні в Україні вже працює система електронної взаємодії органів виконавчої влади (СЕВ ОБВ), яка де факто замінила послугу електронної реєстрованої доставки, описану в законі України Про електронні довірчі послуги (аналог eDelivery). Тобто вона виконує функцію юридично значущого обміну електронними документами, але лише між юридичними особами, бо фізичні особи не мають доступу до цього сервісу. Також враховуючи досвід інтеграції бізнес-реєстрів країн-членів ЄС, Україна не може використовувати СЕВ ОБВ для надсилання інформації про бізнес у європейські органи, оскільки згідно Регламенту (ЄС) № 910/2014 єдиний механізм юридичного визнання послуг реєстрованої доставки (юридично значущого електронного обміну) – це eDelivery.

Для підписання та валідації електронних документів на сайті Центрального засвідчувального органу (ЦЗО) доступний сервіс валідації та перевірки еДок, проте він дозволяє накласти на електронний документ лише один підпис або одну печатку та не надає звіту про валідацію ЕЦП у відповідності до європейських стандартів.

Все це значно обмежує можливість будь-кого (громадянина, представника бізнесу чи органів публічної влади) обмінюватися будь-якими юридично значущими електронними документами з використанням юридично значущої електронної пошти, таким чином зводячи нанівець закладені в законі “Про довірчі послуги” євроінтеграційні механізми.

### *3.4 Стан сфери електронного урядування і електронних послуг в Україні*

Нарешті, для аналізу стану електронного урядування та електронних послуг в Україні, доцільно використати дані так званого індексу розвитку електронного урядування EGDІ – започаткованого ще у 2001 році Організацію об'єднаних націй (ООН) дослідження, за допомогою якого вона регулярно відстежує розвиток у сфері еУрядування серед всіх своїх 193 держав-членів.

Цей рейтинг надає індикативну оцінку ефективності національних урядів у порівнянні один з одним, тобто не в абсолютних, а у відносних значеннях. Кожні два роки в опитуванні оцінюються технічні особливості національних веб-сайтів, а також політики та стратегії електронного урядування, що застосовуються при наданні електронних послуг в цілому в кожній країні та в окремих секторах її економіки. Результати подаються у вигляді таблиць та набору значень індексів, нормалізованих за шкалою від 0 до 1 (чим ближче значення до 1, тим вищий рівень розвитку).

Математично, індекс розвитку електронного урядування EGDI (E-Government Development Index) – це середньозважена нормалізована оцінка таких трьох найважливіших показників електронного урядування:

- обсягу та якості онлайн-послуг OSI (Online Service Index);
- індексу телекомунікаційної інфраструктури ТІІ (Telecommunication Infrastructure Index);
- властивим кожній країні людським капіталом, вираженим у вигляді індексу людського капіталу НСІ (Human Capital Index).

За цим показником цифровізації взаємодії громадян з державою Україна посідає лише 82 місце серед 193 країн світу, а отже значно відстає від своїх найближчих сусідів (для порівняння Росія посідає 32 місце, Польща – 33, Білорусь – 38, Угорщина – 45, Румунія – 67).

Зі своїм показником індексу електронного урядування у розмірі 0,6165 Україна разом з іншими 70 країнами-членами ООН потрапила до групи з високим рівнем EGDI (від 0,5 до 0,75). Як видно з інфографіки на рис. 5, при дуже високому рівні індексу людського капіталу НСІ (0,8436) Україна помітно відстає у показниках індексу онлайн-послуг OSI (0,5694) та особливо індексу телекомунікаційної інфраструктури ТІІ (0,4364), потрапивши з останнім до групи з середніми показниками (від 0,25 до 0,5).

Це свідчить про те, що в Україні багато людей не можуть скористатися усіма можливостями і перевагами цифровізації країни через т розвиток ІКТ-інфраструктури та низьку доступність електронних послуг. Ці недоліки можуть вплинути на подальший розвиток електронного урядування, оскільки темпи інновацій в технології в інших країнах світу весь час посилюються. Для того, щоб побудувати добре функціонуючий електронний уряд, Україні необхідно інтенсифікувати інвестиції в телекомунікаційну інфраструктуру та онлайн-послуги.

## 2018 EGDI

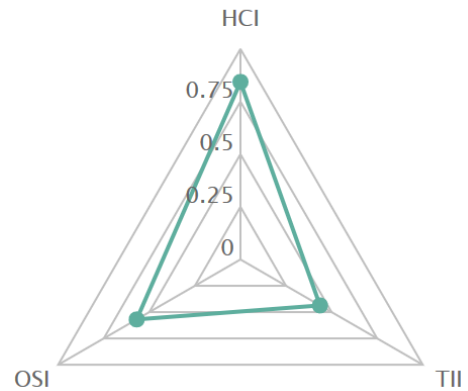
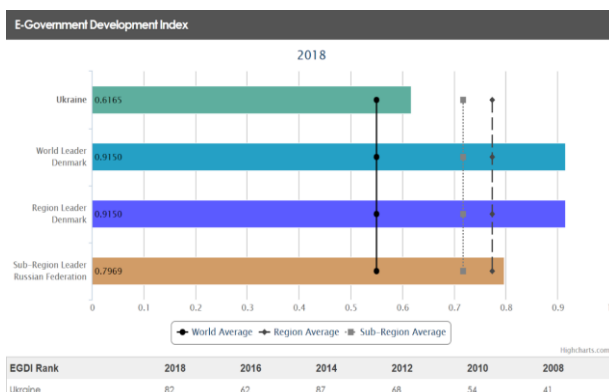


Рис. 3. Рівень індексу розвитку електронного урядування EGDI та його основних складових (OSI, HCI та ТІІ) в Україні у 2018 році

Для наочної ілюстрації стану електронних послуг, доступних в Україні, охарактеризуємо близько десятка з тих, що увійшли до списку найпоширеніших у світі онлайн-послуг за даними дослідження індексу EGDI за 2018 рік:

- 1) оплата за комунальні послуги (надається в 140 країнах);
- 2) подання декларації з податку на прибуток (у 139 країнах);
- 3) реєстрація нового підприємства (у 126 країнах);
- 4) реєстрація особи при народженні (у 86 країнах);
- 5) реєстрація транспортних засобів в режимі онлайн;
- 6) виплата штрафів онлайн;
- 7) отримання свідоцтва про шлюб і водійських посвідчень, свідоцтв про смерть та особистих посвідчень.

Найбільша кількість різноманітних сервісів існує для тих, хто бажає сплатити за комунальні послуги онлайн. Це зокрема такі комерційні сервіси, як <https://www.easypay.ua>, <https://www.ipay.ua/>, <https://www.portmone.com.ua> тощо, або банківські сервіси, наприклад, <https://www.privat24.ua/> від Приватбанку. Проте ідентифікація при вході в ці системи зазвичай здійснюється за допомогою номеру мобільного телефону (або адреси електронної пошти) та пароллю, а не за допомогою ЕЦП.



Подати декларацію з податку на прибуток можна через «Електронний кабінет платника податків»<sup>2</sup>. Саме на цьому ресурсі користувач має можливість пройти ідентифікацію за допомогою ЕЦП при вході у свій особистий кабінет і, як свідчить інструкція користувача, має можливість створити, подати та підписати за допомогою ЕЦП податкову декларацію про майновий стан і доходи громадян (форма F0100210 з групи «F01 Прибуток»). Подання інших звітних документів потребує наявності чинного договору про визнання електронної звітності або прийнятої заяви про приєднання до договору про визнання електронних документів, форма яких визначена Порядком обміну електронними документами з контролюючими органами Міністерства фінансів України. Підписати цей договір та прийняти заяву також можна, не виходячи з «Електронного кабінету платника податків».

Інші електронні послуги на сьогодні в Україні пропонують різні сервіси:

- Кабінет електронних сервісів Міністерства юстиції України та застосування "ДІЯ";
- Веб-портал звернення у сфері державної реєстрації актів цивільного стану;
- Міністерство соціальної політики України;
- Головний сервісний центр МВС України;
- Єдиний веб-портал органів виконавчої влади України;
- Урядовий портал Єдиний веб-портал органів виконавчої влади України;
- Єдиний державний портал адміністративних послуг;
- інші, наприклад, сервіси Держгеокадастру тощо.

Проаналізувавши їх роботу можна зробити такі висновки щодо надання перелічених вище послуг:

1) Деякі послуги вже доступні онлайн, як то послуга сплати за комунальні послуги чи подання декларації з податку на прибуток, проте для деяких послуг можливе лише подання заяв онлайн та онлайн-запис на прийом, наприклад, у випадку вибору послуг реєстрації нового підприємства, реєстрації транспортних засобів, державної реєстрації шлюбу, реєстрації особи при народженні, отримання свідоцтва про шлюб і водійських посвідчень. Це не повністю відповідає визначенню терміну електронна послуга, наданому в законі України Про електронні довірчі послуги (електронна послуга - будь-яка послуга, що надається через інформаційно-телекомунікаційну систему).

2) Для отримання послуг не завжди використовується ідентифікація за допомогою ЕЦП, яка є більш надійним способом, ніж ідентифікація за допомогою номера мобільного телефону та пароллю.

3) Не всі існуючі ресурси-агрегатори електронних послуг однаково корисні і дійсно дають змогу отримати відповідну послугу онлайн.

4) Пошук електронної послуги або інформації про те, як її отримати, відбувається не за один клік, іноді доводиться переглядати цілу низку категорій та підкатегорій або чітко знати, вибір якого пункту меню

дозволить отримати необхідний результат.

### 3.5 *Перепони, що заважають використовувати будівельні блоки eSignature та eID в Україні*

До основних блокерів цифрового безвізу можна віднести:

- 1) зарегульованість сфери;
- 2) відсутність інтеоперабельності;
- 3) відсутність чіткої державної політики щодо використання всього комплексу електронних довірчих послуг.

**Зарегульованість сфери.** Зарегульованість не дає нам можливість залучити європейські органи з оцінки відповідності з метою акредитації-сертифікації українських надавачів довірчих послуг вимогам стандартів ЄС.

На сьогодні в Україні прийнято національне законодавство, що регулює надання кваліфікованих електронних довірчих послуг. Першоджерелом національного законодавства є Закон України «Про електронні довірчі послуги», що відповідає Регламенту 910/2014 ЄС.

Законом визначено повноваження спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації у сферах електронних довірчих послуг та електронної ідентифікації (далі – ДСС). Одним із повноважень ДСС згідно з цим Законом є встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації. на сьогодні вказане питання законодавчо не визначено, що, в свою чергу, порушує положення розділу VII «Прикінцеві та перехідні положення» Закону України «Про електронні довірчі послуги», оскільки такі вимоги мали бути встановлені до 05.10.2018.

19.09.2018 ДСС було опубліковано проект наказу ДСС «Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації», що передбачає впровадження двох систем захисту інформації.

Так, відповідно до пункту 2 Вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації, що пропонується затвердити вказаним проектом наказу, безпека інформаційних ресурсів надавача та відокремлених пунктів реєстрації досягається шляхом впровадження системи управління інформаційної безпеки (далі – СУІБ) та комплексної системи захисту інформації (далі – КСЗІ) інформаційно-телекомунікаційної системи (далі – ІТС) з підтвердженою відповідністю.

Відповідність КСЗІ ІТС вимогам законодавства у сфері захисту інформації, в свою чергу, підтверджується атестатом відповідності та позитивним експертним висновком за результатами державної експертизи в сфері технічного захисту інформації,

виданим підрозділом Держспецзв'язку, підприємства, установи або організації, які проводитимуть експертизу (далі – Організатор експертизи) та затвердженням Головою Держспецзв'язку.

Таким чином потенційно може скластися ситуація, коли вимоги однієї системи інформаційної безпеки протирічтимуть вимогам іншої, тобто потенційні надавачі електронних довірчих послуг не матимуть змоги виконати вимоги щодо безпеки таких послуг, а відповідно створюються непереборні перепони для інтеграції до європейського цифрового ринку, зокрема в частині підписання Угоди про взаємне визнання електронних довірчих послуг. Разом з тим, створюються бар'єри виходу на ринок електронних довірчих послуг та поле для порушення законодавства про захист економічної конкуренції з боку органу влади та здійснення корупційних діянь. Варто відмітити, що на сьогодні, згідно статистики Центрального засвідчувального органу, переважну кількість клієнтів, які отримують електронні довірчі послуги, обслуговують державні кваліфіковані надавачі електронних довірчих послуг.

Отже замість використання системи СУІБ, яка визнається в ЄС, український законодавець намагається створити додаткові перешкоди (зарегулювати) ринок довірчих послуг, паралельно вимагаючи подвійну “сертифікацію” згідно КСЗІ, яка НЕ визнана в ЄС. Тобто нині відсутні реальні кроки у сторону реформування сфери згідно кращих міжнародних практик.

**Відсутність інтероперабельності.** Відсутність інтероперабельності на практиці можна продемонструвати на прикладі критичної складової довірчих послуг – регулюванні надійних носіїв, продовжуємо цю тему після розділу “зарегульованості”.

Засіб кваліфікованого електронного підпису чи печатки (надійний носій) - це апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам Закону України “Про електронні довірчі послуги”. Простіше кажучи, це засіб, який захищає “знання” (особистий ключ) його власника про те, як створити цифровий підпис та печатку. Тобто якщо підписувач зберігає “знання” на флешці, їх можна скопіювати та підписатися “за нього” без його згоди. Надійні носії мають апаратний (на рівні комп'ютерного чіпу) захист цього “знання” і дозволяють лише підписатися (накласти підпис), а НЕ скопіювати підпис.

Для кращого розуміння проблеми, варто висвітлити ситуацію з використанням ЕЦП/КЕП та захищених носіїв особистого ключа, яка торкається майже всього бізнесу (рис. 3).

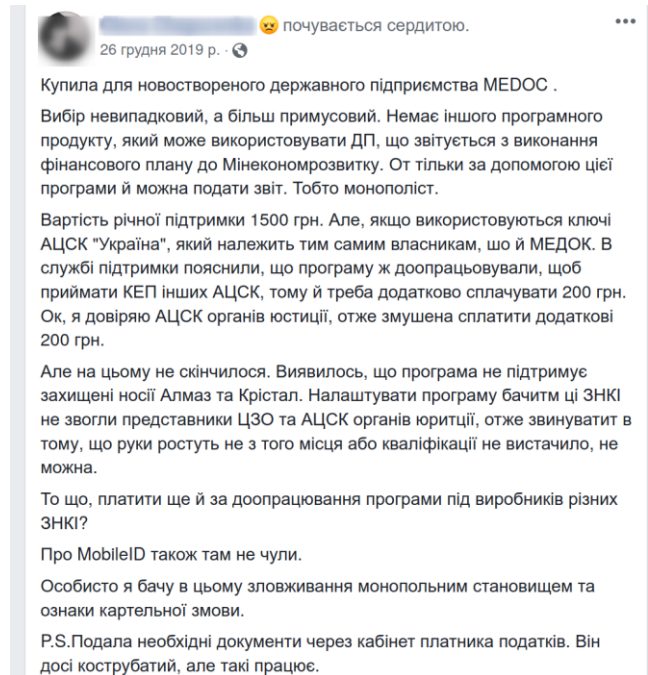


Рис. 3. Коментар щодо використання надійних засобів цифрового підпису

Розглянемо проблеми інтероперабельності (функціональної сумісності) на цьому прикладі. По перше, регулятори в особі Міністерства Цифрової Трансформації України та ДСС досі не регулюють стандарти API (програмні інтерфейси) до захищених носіїв особистих ключів на базі міжнародних стандартів pkcs#11 + pkcs#15. В ідеалі вони мали б створити бібліотеки з відкритим кодом для українських криптографічних алгоритмів.

По друге, центральні органи виконавчої влади досі не інтегрували MobileID та підписи на базі європейських алгоритмів ECDSA у свої сервіси. Прикладом є неможливість підписання податкової звітності європейським алгоритмом цифрового підпису ECDSA із використанням MobileID для подачі до Державної податкової служби України. MobileID є надійним носієм особистого ключа електронного цифрового підпису (особистий ключ зберігається на криптопроцесорі сім-карти), його масове застосування в Україні значно підвищило б рівень кіберзахисту громадян, бізнесу та держави за помірні кошти.

По третє, виробники захищених носіїв через відсутність вимог API надійних носіїв від держави, змушують виробників програмних продуктів, які використовують електронний цифровий підпис, витрачати значний час на інтеграцію виключно їхніх носіїв до програмного забезпечення. Як результат розробники програм бухгалтерської звітності підтримують лише частину “сертифікованих державою” надійних носіїв. Наявність стандартного API надійних засобів дозволила б розробникам використовувати бібліотеки з відкритим кодом чи універсальні бібліотеки для інтеграції з усіма “сертифікованими державою” надійними носіями без додаткових зусиль.

По-четверте, постачальники послуг електронної звітності, які (і тут можливо доцільно вимагати в

"агентських" договорів між державною податковою службою та постачальником послуг електронної звітності), мають підтримувати API надійних носіїв, а не конкретні носії та сервіси, на кшталт MobileID, для уникнення проблем, коли носії не працює із програмою.

**Відсутність чіткої державної політики щодо використання всього комплексу електронних довірчих послуг.** З одного боку, на своїй сторінці у Фейсбук Міністерство цифрової трансформації України оприлюднило таке повідомлення: "Україну обрано для участі в пілотних проектах для транскордонного електронного підпису. Ви часто питаєте, чи можна укласти контракти за допомогою КЕПу з іноземними компаніями. Мінцифра працює, щоб зробити це можливим.

Ось один із кроків у цьому напрямку.

Україну обрано серед країн Східного Партнерства ЄС та запрошено до участі в пілотних проектах по електронному підпису. Відбір проводився на основі оцінки адаптації українського законодавства та технічної реалізації вимог у сфері електронних довірчих послуг.

Ціль пілота – досягнути технічну транскордонну інтероперабельність кваліфікованих електронних підписів. Це надасть можливість підписувати угоди та інші документи з іноземними компаніями за допомогою електронного підпису. Зокрема, Україна тестуватиме е-підписи на реальних прикладах застосування в Естонії та Молдові.

Цим кроком ми наближуємо нашу інфраструктуру до ЄС. І не лише виконуємо наші зобов'язання за Угодою про асоціацію з ЄС, а й використовуємо максимум наявних можливостей європейської інтеграції."

З іншого боку, малий та середній бізнес немає освітніх джерел для роботи з електронними контрактами, які стають критично важливою складовою українського бізнесу в умовах пандемії.

Про скепсис щодо використання електронних первинних документів було заявлено на прес-конференції в УНІАН на тему: «Бізнес та юридично значущі електронні документи – реалії», на якій директор податково-юридичного департаменту компанії «Делойт» Дмитро Павленко зазначив: "На сьогодні, на жаль, бізнес досить скептично ставиться до можливості використання електронних документів".

Адвокат і партнер КМ Партнери Шемяткін Олександр прокоментував проблеми листування із податковою на прикладі (паперового) договору про визнання цифрових підписів між податковою та бізнесом, коли податкова в певних випадках розриває договір про визнання та ігнорує електронні документи підписані цифровим підписом зі сторони бізнесу.

Скепсис пов'язаний із життєвим циклом електронних документів та взагалі із визначенням об'єкту "електронний документ". Наразі пересічний громадянин не може чітко описати процедуру створення електронного документу та як його передати в електронному вигляді в органи публічної влади, на контрасті з паперовим документом. Аналогічно органи публічної влади не мають

а ні освітніх курсів, а ні чіткого розуміння роботи з електронним документом.

І, наостанок, перші особи держави від Президента (який, до речі, отримав внутрішній паспорт у вигляді картки із кваліфікованим цифровим підписом) до канцелярій органів місцевого самоврядування не заохочують громадян та бізнес ввести переписку в юридично значущому цифровому середовищі, за допомогою електронних документів із юридично значущими електронними підписами та печатками з використанням реєстрованої електронної доставки, яка гарантує юридично значущі докази відправки та отримання листів.

Поки перші особи держави та ключові органи державної влади, які займаються цифровізацією країни, послуговуються паперовим документообігом, доти бізнес та громадяни будуть скептично ставитися до електронних документів і електронних сервісів.

#### IV. ВИСНОВКИ

Отже для усунення перепон, що заважають Україні піти найкоротшим шляхом для створення комерційної інфраструктури спільного цифрового ринку та запровадити європейське програмне забезпечення для застосування юридично значущих довірчих послуг на європейських стандартах, необхідно:

- сприяти проведенню перевірки експертами ЄС на відповідність Регламенту Національної системи електронних довірчих послуг з метою підготовки угоди про взаємне визнання електронних довірчих послуг між Україною та ЄС;
- визначити на рівні національного законодавства норму, яка забезпечить визнання документів про відповідність у сферах електронних довірчих послуг та інформаційної безпеки, виданих органами з оцінки відповідності, що акредитовані у державах-членах ЄС, як це робиться такими державами-членами;
- забезпечити інтероперабельність надання електронних довірчих послуг через застосування безкоштовного програмного забезпечення Європейської комісії (наприклад, вже згаданої вище бібліотеки DSS або проекту з відкритим кодом Domibus для реалізації послуг eDelivery), для розбудови цифрової інфраструктури довіри в органах публічної влади;
- забезпечити підтримку технології MobileID в системах електронного документообігу органів державної влади з метою взаємодії громадян, бізнесу та держави;
- розробити освітні курси з застосування електронних довірчих послуг, на кшталт "Вступ до електронного документообігу";
- сприяти популяризації електронних довірчих послуг через перших осіб держави, які мають почати активно використовувати довірчі послуги та електронні документи при виконанні своїх офіційних обов'язків.

## ЛІТЕРАТУРА

- [1] Why we need a Digital Single Market – [https://ec.europa.eu/commission/publications/why-we-need-digital-single-market\\_en](https://ec.europa.eu/commission/publications/why-we-need-digital-single-market_en)
- [2] A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen – [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_15\\_4919](https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4919)
- [3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC – [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG)
- [4] Learn about eIDAS – <https://ec.europa.eu/digital-single-market/en/learn-about-eidas>
- [5] Executive Summary: The Advantages, Economics and Value of Reuse – <https://www.gartner.com/en/documents/1406319/executive-summary-the-advantages-economics-and-value-of->
- [6] Andrea Servida. From Pilots to Reality – [https://www.esens.eu/sites/default/files/1.\\_esens-march3.pdf](https://www.esens.eu/sites/default/files/1._esens-march3.pdf)
- [7] Digital Signature Service (DSS) – [https://joinup.ec.europa.eu/sd-dss/webapp-demo/doc/dss-documentation.html#\\_purpose\\_of\\_the\\_document](https://joinup.ec.europa.eu/sd-dss/webapp-demo/doc/dss-documentation.html#_purpose_of_the_document)
- [8] Estonia opened up its service portals with CEF – <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/11/08/Estonia+opened+up+its+service+portals+with+CEF+-+expanding+3%2C500+services+across+Europe>
- [9] Гречко А.В., Мелашенко А.О., Таран С.В. Електроні довірчі послуги – основа бізнес-довіри / Гречко А.В., Мелашенко А.О., Таран С.В. // Науковий журнал. Щорічник. "Наукові записки НаУКМА. Комп'ютерні науки", Том 1. – 2018. – С. 50-53.
- [10] Гречко А.В., Мелашенко А.О., Таран С.В. Електроні довірчі послуги – основа бізнес-довіри / Гречко А.В., Мелашенко А.О., Таран С.В. // Науковий журнал. Щорічник. "Наукові записки НаУКМА. Комп'ютерні науки", Том 1. – 2018. – С. 50-53.
- [11] Гречко А.В., Мелашенко А.О., Таран С.В. Електроні довірчі послуги – основа бізнес-довіри / Гречко А.В., Мелашенко А.О., Таран С.В. // Науковий журнал. Щорічник. "Наукові записки НаУКМА. Комп'ютерні науки", Том 1. – 2018. – С. 50-53.