

Договір про надання ідентифікаторів доступу до Єдиних та Державних реєстрів

м. Київ

Державне підприємство «Національні інформаційні системи» (надалі – Підприємство), в особі генерального директора Лур'є Станіслава Сергійовича, який діє на підставі Статуту, з однієї сторони, та

Користувач¹, в особі уповноваженого представника, який підписав заяву про приєднання до цього Договору з іншої сторони, надалі разом – Сторони, уклали цей Договір про надання ідентифікаторів доступу до Єдиних та Державних реєстрів (далі – Договір) про нижченаведене.

1. Предмет Договору та загальні умови

- 1.1. Предметом цього Договору є здійснення Підприємством організаційних заходів щодо надання працівникам Користувача, які відповідно до законодавства мають право доступу до Єдиних та Державних реєстрів, створення та забезпечення функціонування яких належить до компетенції Міністерства юстиції України (далі - Системи), ідентифікаторів (логіну та паролю) доступу до Систем, у кількості, що відповідає кількості працівників Користувача, зазначених у письмовому замовленні, що подається Користувачем за формою, встановленою у Додатку 2 до Договору, з метою здійснення ними повноважень, передбачених чинним законодавством України.
- 1.2. Доступ до Систем надається працівникам Користувача з використанням ідентифікаторів доступу та електронного цифрового підпису, сумісного з програмним забезпеченням Систем.
- 1.3. Користувач самостійно здійснює дії, пов'язані з отриманням послуг електронного цифрового підпису в Акредитованому центрі сертифікації ключів. Підприємством, за зверненням Користувача, надається консультативна інформація щодо порядку отримання послуг електронного цифрового підпису в Акредитованому центрі сертифікації ключів органів юстиції України.

2. Визначення термінів

- 2.1. У цьому Договорі терміни вживаються в такому значенні:
 - 2.1.1. **Акредитований центр сертифікації ключів** – юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги електронного цифрового підпису, засвідчила свій відкритий ключ у центральному засвідчувальному органі та пройшла акредитацію відповідно до порядку, визначеного законодавством.
 - 2.1.2. **Електронний цифровий підпис** – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.
 - 2.1.3. **Особистий ключ** – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.
 - 2.1.4. **Компрометація ідентифікаторів доступу** – будь-яка подія та/або дія (зокрема, втрата, розголошення, крадіжка, несанкціоноване копіювання), що призвела або може призвести до несанкціонованого використання ідентифікатора доступу.
 - 2.1.5. **Ідентифікатор доступу** – це логін (реєстраційне ім'я, що складається з буквених та цифрових символів та використовується для ідентифікації при отриманні доступу до Систем) та пароль (секретний набір символів, який використовується для аутентифікації належності пред'явленого особистого логіна для доступу до Систем).
- 2.2. Інші поняття і терміни вживаються в цьому Договорі в значеннях, визначених законодавством України.

¹ Назва органу державної влади, органу місцевого самоврядування зазначається у заяві про приєднання до цього Договору.

3. *Обов'язки та права Сторін*

3.1. *Обов'язки Підприємства:*

- 3.1.1. Надати працівникам Користувача ідентифікатори доступу до Систем в кількості, що відповідає кількості працівників Користувача, зазначених у замовленні, форма якого наведена в Додатку 2 до цього Договору, що надається Користувачем.
- 3.1.2. За письмовим повідомленням Користувача, здійснити заходи щодо скасування ідентифікаторів доступу до Систем, які були надані Підприємством співробітнику Користувача.
- 3.1.3. Забезпечити безперешкодний доступ працівників Користувача до Систем у відповідності до їх прав, та за умов використання ними ідентифікаторів доступу відповідно до вимог законодавства та цього Договору.

3.2. *Обов'язки Користувача:*

- 3.2.1. Забезпечити своєчасне надання Підприємству письмових замовлень за формою, встановленою Додатком 2 до цього Договору, на необхідну кількість ідентифікаторів доступу.
- 3.2.2. Забезпечити безумовне дотримання вимог Регламенту Акредитованого центру сертифікації ключів працівниками Користувача, які для роботи з Системами отримали особистий ключ та посиленний сертифікат ключа.
- 3.2.3. Забезпечити збереження працівниками Користувача ідентифікаторів доступу, особистих ключів та паролів до них у таємниці та забезпечити недопущення їх використання іншими особами. У випадку виявлення факту використання третіми особами ідентифікаторів доступу та/або особистих ключів, або при виникненні підозри щодо використання ідентифікаторів доступу та/або особистих ключів третіми особами – негайно вжити всіх необхідних заходів для припинення факту такого використання.
- 3.2.4. Забезпечити безумовну заміну працівниками тимчасового паролю на власний із дотриманням вимог безпеки, встановлених в Системах для паролю, під час першого входу до Систем.
- 3.2.5. Не допускати використання ідентифікаторів доступу та/або особистого ключа у разі їх компрометації.
- 3.2.6. Негайно, але не пізніше 2 (двох) робочих днів, письмово повідомляти Підприємство про необхідність скасування ідентифікаторів доступу до Систем співробітникам Користувача, які припинили працювати з Системами, а також, у разі необхідності, негайно звернутися до Акредитованого центру сертифікації ключів для скасування відповідного посиленого сертифіката відкритого ключа.
- 3.2.7. Забезпечити кваліфікований персонал для роботи з Системами.
- 3.2.8. Не передавати ні право, ні можливість доступу до Систем третім особам, окрім як співробітникам Користувача, зазначеним у замовленні, форма якого наведена у Додатку 2 до цього Договору.
- 3.2.9. Якщо Підприємству стало відомо про факт передачі працівником Користувача права або можливості доступу до Систем третім особам, Підприємство має право призупинити доступ до Систем такому працівнику Користувача.
- 3.2.10. Надавати Підприємству всю необхідну інформацію, пов'язану з виконанням умов даного Договору.
- 3.2.11. Користуватися Системами у відповідності до вимог, встановлених чинним законодавством України.
- 3.2.12. Користуватися відомостями, отриманими при роботі з Системами, у відповідності до вимог нормативно-правових актів та у межах повноважень, визначених законодавством.
- 3.2.13. Вжити заходів для забезпечення зберігання, запобігання несанкціонованому доступу та поширенню персональних даних, отриманих у зв'язку з користуванням Системами, відповідно до законодавства.
- 3.2.16. Не надавати третім особам за їх зверненням інформацію, отриману у зв'язку з користуванням Системами, окрім випадків визначених законодавством.
- 3.2.17. Забезпечити захист комп'ютерного робочого місця співробітника Користувача, якому Підприємством забезпечено доступ для роботи із Системами, відповідно до вимог чинного законодавства у сфері захисту інформації.

3.3. *Підприємство має право*

- 3.3.1. Перевіряти додержання Користувачем умов цього Договору та дотримання працівниками Користувача порядку роботи з Системами.
- 3.3.2. У разі невиконання або неналежного виконання Користувачем умов цього Договору, вимагати усунення порушень, або призупинити дію Договору, або відмовитися від виконання Договору та розірвати Договір в односторонньому порядку.
- 3.3.3. Отримувати від Користувача інформацію, пов'язану з виконанням умов цього Договору, у тому числі, документи, які підтверджують повноваження Користувача, визначені законодавством, у зв'язку із здійсненням яких Користувач має право доступу до Систем.
- 3.3.4. Скасовувати ідентифікатори доступу, що були надані працівникам Користувача для роботи з Системами, які не використовуються протягом 3 (трьох) місяців.
- 3.3.5. Тимчасово призупинити доступ до Систем працівникам Користувача на письмову вимогу правоохоронних органів, або щодо яких надійшла інформація про компрометацію їх ідентифікаторів доступу або особистих ключів.
- 3.3.6. У разі порушення Користувачем вимог підпункту 3.2.8 та пункту 6.11 розділу 6 Договору, Підприємство має право зупинити надання можливості користування Системами працівникам Користувача.
- 3.3.7. У випадку виникнення підозри щодо вірусних атак з комп'ютерного робочого місця Користувача, Підприємство має право призупинити надання можливості користування Системами працівникам Користувача до повного усунення загрози.
- 3.3.8. Підприємство має право направляти Користувачу електронні повідомлення з питань, що стосуються роботи Систем, або перерв у їх роботі тощо, які за статусом прирівнюються до офіційних письмових повідомлень Підприємства.

3.4. Користувач має право

- 3.4.1. Забезпечити використання працівниками Користувача ідентифікаторів доступу до Систем з метою здійснення повноважень, визначених законодавством, у порядку та на підставах, встановлених чинним законодавством України.
- 3.4.2. Вимагати від Підприємства виконання зобов'язань за цим Договором.

4. Відповідальність Сторін

- 4.1. У випадку невиконання або неналежного виконання зобов'язань, що виникають з цього Договору, Сторони несуть відповідальність, визначену цим Договором, а також згідно з чинним законодавством України.
- 4.2. Користувач несе відповідальність перед третіми особами згідно з чинним законодавством України за втрату його працівниками ідентифікаторів доступу до Систем, носія ключової інформації з особистим ключем та паролем до нього, внаслідок чого відбулися несанкціоновані дії з інформацією в Системах від імені його працівників, за знищення особистого ключа з носія ключової інформації та втрату пароля захисту особистого ключа, а також за недостовірність інформації, яку вносять до Систем працівники Користувача, за помилки, допущені ними при роботі з Системами, а також за невиконання інших обов'язків, визначених цим Договором, що призвело до завдання шкоди третім особам.
- 4.3. Відповідальність за неякісне надання послуг електронного цифрового підпису працівникам Користувача несе Акредитований центр сертифікації ключів.
- 4.4. Підприємство несе відповідальність за незабезпечення встановленого рівня конфіденційності технічних даних щодо ідентифікаторів доступу працівників Користувача в Системах, а також за розголошення персональних даних працівників Користувача, окрім випадків, передбачених законодавством.
- 4.5. Подаючи заяву про приєднання до цього Договору, Користувач підтверджує наявність у нього повноважень визначених законодавством, у зв'язку із виконанням яких він має право доступу до Систем. Користувач відповідає за повноту та достовірність інформації наданої в заяві про приєднання до цього Договору, у тому числі про віднесення працівників Користувача до кола осіб, які відповідно до законодавства мають право доступу до Систем.

5. Підстави звільнення Сторін від відповідальності

- 5.1. Сторони звільняються від відповідальності за порушення зобов'язань за цим Договором, якщо таке порушення є наслідком дії обставин непереборної сили або випадку, і якщо Сторона доведе існування таких обставин.

- 5.2. Під непереборною силою у цьому Договорі розуміються будь-які надзвичайні події зовнішнього щодо Сторін характеру, які виникають без вини Сторін, поза їх волею або всупереч волі чи бажанню Сторін і які не можна за умови вжиття звичайних для цього заходів передбачити та не можна при всій турботливості та обачності відвернути (уникнути), включаючи (але не обмежуючись) стихійні явища природного характеру (землетруси, пожежі, бурі, нагромадження снігу або ожеледь, повені, урагани, руйнування в результаті блискавки тощо), лиха біологічного, техногенного та антропогенного походження (вибухи, пожежі, вихід з ладу машин й обладнання, масові епідемії, епізоотії, епіфітотії тощо), обставини суспільного життя (війна, загроза війни, революції, заколоти, повстання, воєнні дії, блокади, громадські хвилювання, прояви тероризму, вибухи, масові страйки та локаути, бойкоти тощо), а також видання заборонних або обмежуючих актів органів державної влади чи місцевого самоврядування, інші законні або незаконні заборонні чи обмежуючі заходи названих органів, які унеможливають виконання Сторонами цього Договору або тимчасово перешкоджають такому виконанню.
- 5.3. Під випадком у цьому Договорі розуміються будь-які обставини, які не вважаються непереборною силою за цим Договором і які безпосередньо не обумовлені діями Сторін та не пов'язані із ними причинним зв'язком, які виникають без вини Сторін, поза їх волею або всупереч волі чи бажанню Сторін і які не можна за умови вжиття звичайних для цього заходів передбачити та не можна при всій турботливості та обачності відвернути (уникнути).
- 5.4. При виникненні обставин дії непереборної сили або випадку строк виконання зобов'язань відкладається на строк дії таких обставин.
- 5.5. Сторона, для якої є неможливим виконання зобов'язань за цим Договором внаслідок дії непереборної сили або випадку, повинна при першій можливості повідомити іншу Сторону про настання, ймовірну тривалість та закінчення строку таких дій.
- 5.6. Доказом існування обставин непереборної сили та строку їх дії є належним чином оформлені довідки відповідних державних органів.
- 5.7. Випадок підтверджується фото-, відеозйомками, свідченнями третіх осіб, відомостями, розміщеними в ЗМІ тощо.
- 5.8. З моменту припинення дії непереборної сили або випадку Сторони зобов'язані виконати передбачені цим Договором зобов'язання.
- 5.9. У випадку, якщо обставини непереборної сили або випадку тривають більше одного календарного місяця, кожна із Сторін має право відмовитись від Договору, попередивши про це іншу Сторону за 10 календарних днів до бажаної дати припинення дії Договору.

6. Працівникам Користувача забороняється

- 6.1. Модифікувати програмне забезпечення Систем, у тому числі вносити зміни в об'єктний код або дані програм.
- 6.2. Розповсюджувати або передавати третім особам ідентифікатори доступу до Систем, особисті ключі, паролі та коди доступу до них.
- 6.3. Дезасемблювати, декомпілювати (змінювати об'єктний код в вихідний текст) програми, бази даних та інші компоненти програмного забезпечення Систем.
- 6.4. Створювати умови для несанкціонованого використання програмного забезпечення Систем, а також ідентифікаторів доступу та особистих ключів третіми особами.
- 6.5. Видаляти будь-які компоненти зі складу програмного забезпечення Систем.
- 6.6. Виконувати автоматичну авторизацію в Системах.
- 6.7. Впроваджувати програмні засоби для автоматичної ідентифікації та автентифікації в Системах.
- 6.8. Впроваджувати програмні засоби для Автоматичного внесення даних до Систем або автоматичного отримання даних з Систем.
- 6.9. Зберігати ідентифікатори доступу та особисті ключі на файловій системі комп'ютера працівника, у сторонньому програмному забезпеченні, на іншому носії або в іншому місці, доступному третім особам.
- 6.10. Накопичувати та зберігати дані з Систем на файловій системі комп'ютера працівника.
- 6.11. Користувач здійснює необхідні заходи щодо недопущення вчинення його працівниками дій, зазначених у п.п. 6.1 – 6.10 цього Договору.
- 6.12. У разі порушення працівником Користувача вимог п.п. 3.2.2, 3.2.8 та п.п. 6.1 – 6.10 цього Договору, Підприємство має право зупинити доступ до Систем такому працівнику.

7. Строк дії та пролонгація Договору

- 7.1. Цей Договір набирає чинності з дати прийняття Підприємством в особі відповідної філії від Користувача заповненої належним чином заяви про приєднання до цього Договору і діє протягом одного року до 31 грудня 2016 року.
Якщо жодна із Сторін не заявить про припинення дії цього Договору за 30 (тридцять) днів до закінчення терміну його дії, тобто до 01 грудня поточного року, то Договір вважається продовженим на кожний наступний рік на таких самих умовах.
- 7.2. **Договір може бути розірвано:**
- 7.2.1. за взаємною згодою Сторін, зафіксованою у письмовій формі;
- 7.2.2. з ініціативи однієї із Сторін з обов'язковим попередженням іншої Сторони у письмовій формі не пізніше, як за п'ятнадцять календарних днів до дати розірвання;
- 7.2.3. в односторонньому порядку Підприємством у разі невиконання або неналежного виконання Користувачем умов цього Договору (одностороння відмова від Договору), або у разі істотної зміни обставин, якими Сторони керувалися при укладенні даного Договору.

8. Інші умови

- 8.1. Правовий режим функціонування Систем, а також порядок доступу до Систем регулюється чинним законодавством України, документами Підприємства та цим Договором.
- 8.2. Договір, відповідно до статті 631 Цивільного кодексу України, поширює свою дію на взаємовідносини Сторін, які виникли та діяли до моменту його укладення.
- 8.3. Офіційна інформація Підприємства публікується на офіційному веб-сайті Підприємства за адресою <http://nais.gov.ua>.
- 8.4. Особи, що уклали цей Договір від імені Підприємства та Користувача, погодились, що їх персональні дані, які стали відомі Сторонам в зв'язку з укладанням цього Договору включаються до баз персональних даних Сторін. Представники сторін підписанням цього договору підтверджують, що вони повідомлені про свої права відповідно до ст. 8 Закону України «Про захист персональних даних».
- 8.5. Даний Договір є договором приєднання, та укладається шляхом приєднання Користувача до запропонованого Договору в цілому, при цьому Користувач не може запропонувати свої умови цього Договору. У випадку незгоди зі змістом та формою Договору, чи окремих його положень, Користувач вправі відмовитися від його укладення.
- 8.6. Користувач, працівники якого, на момент подачі заяви про приєднання до цього договору, вже користуються ідентифікаторами доступу до Систем, які видавалися попередніми адміністраторами Систем, разом з заявою про приєднання до цього Договору надсилає розписки про отримання співробітниками Користувача ідентифікаторів доступу до Систем, форма яких встановлена у Додатку 3 до Договору, для проведення переакредитації таких ідентифікаторів.
- 8.7. Форма Заяви про приєднання до умов цього Договору встановлена у Додатку 1.
Форма Замовлення встановлена у Додатку 2.
Форма Розписки про отримання ідентифікаторів доступу до Систем встановлена у Додатку 3.

9. Адреси та банківські реквізити Сторін

Державне підприємство
„Національні інформаційні системи”

Юридична адреса:

04053, Київ, вул. Артема, 73

код ЄДРПОУ 39787008

п/р 26009484744

в АТ „Райффайзен Банк Аваль”

МФО 380805

Статус платника податку на прибуток:

Платник податку на прибуток на загальних умовах.

КОРИСТУВАЧ

Реквізити зазначаються у заяві про приєднання до цього Договору

На бланку Користувача

Вих. № _____ філія
 від _____

(відповідно до регіону місцезнаходження Користувача)

**державного підприємства
 «Національні інформаційні системи»**

**Заява про приєднання
 до Договору про надання ідентифікаторів доступу до Єдиних та Державних реєстрів**

Назва органу державної влади; органу місцевого самоврядування; (заповнюється повністю відповідно до даних, які містяться в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань)

Код ЄДРПОУ										

Юридична адреса Користувача:

Країна	Індекс	Область	Район

Місто (селище)	Вулиця (бульвар, проспект, площа)	буд.	корп.	кв.

Адреса Користувача для листування (вказати за необхідності):

Країна	Індекс	Область	Район	
Місто (селище)	Вулиця (бульвар, проспект, площа)	буд.	корп.	кв.

Додаткові відомості :

Контактний телефон:
Контактна електронна адреса:

Відповідно до статті 634 Цивільного кодексу України шляхом подання цієї Заяви Користувач приєднується до Договору про надання ідентифікаторів доступу до Єдиних та Державних реєстрів (далі - Договір) та його умов, встановлених державним підприємством «Національні інформаційні системи» (далі – Підприємство), розміщеного на офіційному веб-сайті Підприємства за адресою www.nais.gov.ua.

Користувач підписанням цієї Заяви засвідчує, що він ознайомився з умовами Договору, погоджується з ними та зобов'язується їх виконувати, підтверджує наявність у нього повноважень, визначених законодавством, у зв'язку із виконанням яких він має право отримувати доступ до Єдиних та Державних реєстрів (далі - Системи), а також надає згоду (дозвіл) на обробку персональних даних.

Подання цієї Заяви є підставою для здійснення Підприємством організаційних заходів з надання співробітникам Користувача особистих ідентифікаторів доступу до Систем відповідно до законодавства.

Додаток: у випадку підписання заяви НЕ керівником установи, до заяви додаються документи, які підтверджують повноваження підписанта Заяви.

_____ посада

_____ підпис

_____ П.І.Б.

М.П.

НА БЛАНКУ КОРИСТУВАЧА, ЯКИЙ ПРИЄДНАВСЯ ДО ДОГОВОРУ

від « ____ » _____ 20__ р.
вих. № _____

_____ філії
державного підприємства
«Національні інформаційні
системи»

_____ (найменування Користувача)
адреса _____
контактний телефон _____

ЗАМОВЛЕННЯ

3 метою забезпечення належної реалізації положень

(положення законодавства, у зв'язку із реалізацією яких співробітники Замовника мають право доступу до Єдиних та Державних реєстрів)

прошу надати співробітникам _____ (назва Користувача)

(код ЄДРПОУ - _____), що зазначені в цьому замовленні, ідентифікатори доступу до Єдиних та Державних реєстрів (далі – Системи), адміністратором якого є державне підприємство «Національні інформаційні системи» (далі - Підприємство).

Підписуючи це замовлення, Користувач підтверджує, що співробітники, зазначені у цьому замовленні, відповідно до законодавства мають право доступу до Систем, у зв'язку із здійсненням ними повноважень, визначених законодавством України, та володіють навиками роботи з інформаційними системами.

Перелік співробітників

№ з/п	ПІБ співробітника (повністю, відповідно до паспортних даних)	Серія та номер паспорта співробітника	РНОК ПП	Посада	Назва Єдиних та Державних реєстрів до яких отримується доступ	Тип прав доступу до відповідного реєстру	Контактний номер телефону, контактна адреса електронної пошти	Підтвердження згоди на обробку персональних даних* (особистий підпис)
1								
2								
...								

* - Цим підписом підтверджую згоду (надаю дозвіл) на обробку моїх персональних даних для отримання доступу до Систем.

_____ (посада)

_____ (підпис, М.П.)

_____ (П.І.Б.)

РОЗПИСКА

Про переакредитацію користувача Єдиного державного реєстру юридичних осіб та фізичних осіб – підприємців та громадських формувань

Я, _____
прізвище, ім'я та по батькові

назва організації, підприємства, установи, посада

відповідно до даної розписки отримав(ла) від державного підприємства "Національні інформаційні системи" логін та пароль доступу до Єдиних та Державних реєстрів, з метою здійснення відповідних дій у межах повноважень, визначених нормативно-правовими актами, що регламентують їх функціонування. Навиками роботи з інформаційними системами володію.

діючий логін _____

Зобов'язуюсь не передавати ні логін, ні пароль іншим особам. Також зобов'язуюсь повідомляти Підприємство у випадку підозри або факту доступу інших осіб до автоматизованих систем за моїм логіном та паролем для подальшого закриття доступу.

Зі змістом статей 231, 232, 361-363¹ Кримінального кодексу України та статей 212⁵, 212⁶ Кодексу України про адміністративні правопорушення, за якими настає відповідальність за порушення даного мною зобов'язання ознайомлений(а).

Підпис користувача _____

Дата _____

Додаткові дані:
