ЗАТВЕРДЖЕНО

Наказ Міністерства цифрової

трансформації України

\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_

**РЕГЛАМЕНТ**

**роботи інтегрованої системи електронної ідентифікації**

**І. Загальні положення**

1. Цей Регламент визначає організаційно-методологічні, технічні та технологічні умови функціонування інтегрованої системи електронної ідентифікації (далі – система), вимоги щодо ідентифікації та автентифікації суб’єктів взаємодії під час підключення до системи, процедури захищеного обміну та управління інформаційними потоками під час транскордонної електронної ідентифікації.

2. Дія цього Регламенту поширюється на суб’єктів взаємодії, визначених пунктом 8 Положення про інтегровану систему електронної ідентифікації, затвердженого постановою Кабінету Міністрів України від 19 червня
2019 року № 546 (далі – Положення).

3. У цьому Регламенті терміни вживаються у такому значенні:

єдина інформаційна система МВС – багатофункціональна інтегрована автоматизована система, що безпосередньо забезпечує реалізацію функцій її суб’єктів, інформаційну підтримку та супроводження їх діяльності і становить сукупність взаємозв’язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію, порядок функціонування якої визначено постановою Кабінету Міністрів України від 14 листопада 2018 року № 1024 «Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів»;

Система BankID Національного банку України – національна система електронної дистанційної ідентифікації, порядок функціонування якої визначено постановою Національного банку України від 17 березня 2020 року № 32 «Про затвердження Положення про Систему BankID Національного банку України»;

система електронної ідентифікації операторів мобільного зв’язку Mobile ID – послуга електронної ідентифікації, автентифікації та електронного підпису, яка надається за допомогою технологій стільникового зв’язку, з використанням SIM-картки у мобільному пристрої абонента у якості захищеного носія ключових даних та інфраструктури відкритих ключів України.

Інші терміни вживаються у значеннях, наведених в Цивільному кодексі України, Законах України «Про електронні довірчі послуги», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації», «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус», постановах Кабінету Міністрів України від 08 вересня 2016 року № 606 «Деякі питання електронної взаємодії державних електронних інформаційних ресурсів», від 07 листопада 2018 року № 992 «Про затвердження вимог у сфері електронних довірчих послуг та Порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг», від 19 червня 2019 року № 546 «Про затвердження Положення про інтегровану систему електронної ідентифікації», нормативно-правових актах з питань криптографічного та технічного захисту інформації.

4. Держателем системи є Міністерство цифрової трансформації України:

місцезнаходження (поштова адреса): вул. Ділова, 24, м. Київ, 03150;

код за ЄДРПОУ: 43220851;

адреса електронної пошти: hello@thedigital.gov.ua.

5. Технічним адміністратором системи є державне підприємство «ДІЯ»:

місцезнаходження (поштова адреса): вул. Ділова, 24, м. Київ, 03150;

код за ЄДРПОУ 43395033;

адреса електронної пошти: inbox@diia.gov.ua.

6. Роботу держателя системи організовано в одну робочу зміну з понеділка по четвер з 09:00 до 18:00, обідня перерва – з 13:00 до 13:45; у п'ятницю – з 09:00 до 16:45, обідня перерва – з 13:00 до 13:45.

7. Роботу технічного адміністратора системи з питань приєднання інформаційно-телекомунікаційних систем суб’єктів взаємодії до системи та інформаційна підтримка суб’єктів взаємодії та користувачів системи організовано в одну робочу зміну з понеділка по четвер з 09:00 до 18:00, обідня перерва – з 13:00 до 13:45; у п'ятницю – з 09:00 до 16:45, обідня перерва – з 13:00 до 13:45.

8. Технічна підтримка технічним адміністратором системи суб’єктів взаємодії, інформаційно-телекомунікаційні системи яких приєднано до системи, здійснюється цілодобово.

9. Цей Регламент та зміни до нього розміщуються на вебсайті системи (<https://id.gov.ua>).

10. Система функціонує цілодобово сім днів на тиждень.

**ІІ. Управління та операційний контроль**

1. Система забезпечує реалізацію таких компонентів цільового призначення:

реалізацію регламентних процедур та процесів електронної ідентифікації фізичних та юридичних осіб для отримання ними електронних послуг та сервісів;

забезпечення взаємодії та сумісності із інформаційно-телекомунікаційними системами, які реалізують схеми електронної ідентифікації та інформаційно-телекомунікаційними системами надання електронних послуг та/або сервісів чи потребують електронної ідентифікації;

організаційне та технологічне забезпечення виконання вимог законодавства щодо захисту інформації, кібербезпеки та захисту персональних даних;

інтеграцію з інформаційно-телекомунікаційними системами в рамках транскордонної електронної взаємодії;

інтеграцію інформаційно-телекомунікаційних систем суб'єктів взаємодії електронної ідентифікації.

2. Система складається з сукупності таких функціонально пов'язаних підсистем:

підсистема взаємодії зі схемами електронної ідентифікації кваліфікованих надавачів електронних довірчих послуг;

підсистема взаємодії зі схемами електронної ідентифікації з використанням відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, оформленому особі засобами Єдиного державного демографічного реєстру;

підсистема взаємодії з Системою Bank ID Національного банку України;

підсистема взаємодії з проміжними вузлами схем електронної ідентифікації операторів мобільного зв'язку Mobile ID;

підсистема верифікації відомостей щодо фізичних і юридичних осіб, фізичних осіб - підприємців, які є користувачами системи;

підсистема створення та перевірки кваліфікованого електронного підпису;

підсистема управління;

підсистема захисту інформації.

3. До складу системи входять такі технічні засоби:

сервери ідентифікації;

сервер віртуалізації;

сервери бази даних;

консоль керування серверами;

дисковий масив (система зберігання даних);

комутатори локальної обчислювальної мережі (ЛОМ);

міжмережні екрани (МЕ);

мережні криптомодулі «Гряда-301»;

шлюз захисту «Бар’єр-301»;

блок розподілу живлення (автоматичний перемикач);

робочі станції адміністраторів;

комутатор терміналів;

GSM модем.

4. Система під час функціонування взаємодіє з серверами прикладних систем, користувачами (клієнтами) прикладних систем, інформаційними системами кваліфікованих надавачів електронних довірчих послуг, серверами мобільного підпису (оператора зв’язку), сервером банківської ідентифікації, сервером електронної ідентифікації з використанням відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, оформленому особі засобами Єдиного державного демографічного реєстру, серверами сторонніх інформаційно-телекомунікаційних систем, які потребують електронної ідентифікації, Системою електронної взаємодії державних електронних інформаційних ресурсів, єдиною інформаційною системою МВС, сервером Системи BankID Національного банку України.

5. Всі технічні засоби системи забезпечують можливість діагностування та отримання інформації про стан їх функціонування.

6. Підсистема взаємодії зі схемами електронної ідентифікації кваліфікованих надавачів електронних довірчих послуг забезпечує виконання таких функцій:

автентифікація інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

автентифікація кваліфікованих надавачів електронних довірчих послуг;

автентифікація фізичних осіб та фізичних осіб-представників юридичних осіб, які звертаються до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі (користувачів електронних довірчих послуг), з використанням особистих ключів та сертифікатів відкритих ключів за запитами від інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

захищений обмін інформацією зі схемами електронної ідентифікації кваліфікованих надавачів електронних довірчих послуг;

передача ідентифікаційних даних фізичних осіб та фізичних осіб-представників юридичних осіб (користувачів електронних довірчих послуг), які успішно пройшли процес автентифікації, до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

взаємодія із кваліфікованими надавачами електронних довірчих послуг за протоколами визначення статусу сертифікатів відкритих ключів та (додатково) за протоколом управління сертифікатами.

7. Підсистема взаємодії з Системою BankID Національного банку України забезпечує виконання таких функцій:

автентифікація інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

автентифікація Системи BankID Національного банку України;

захищений обмін інформацією із Системою BankID Національного банку України;

автентифікація фізичних осіб, які звертаються до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі (користувачів платіжних послуг банківських установ), з використанням протоколів банківських систем дистанційного обслуговування;

передача ідентифікаційних даних фізичних осіб, отриманих через Систему BankID Національного банку України, які успішно пройшли процес автентифікації за допомогою банківських систем дистанційного обслуговування, до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

Обмін інформацією під час взаємодії з Системою BankID Національного банку України повинен відповідати специфікаціям взаємодії, які затверджені Національним банком України.

8. Підсистема взаємодії з проміжними вузлами схем електронної ідентифікації операторів мобільного зв’язку MobileID забезпечує виконання таких функцій:

автентифікація інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

автентифікація інформаційно-телекомунікаційних систем, які реалізують схеми електронної ідентифікації операторів мобільного зв’язку MobileID;

захищений обмін інформацією із проміжними вузлами схем електронної ідентифікації операторів мобільного зв’язку MobileID;

автентифікація фізичних осіб та фізичних осіб-представників юридичних осіб, які звертаються до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі (користувачів послуг мобільного зв’язку), з використанням особистих ключів та сертифікатів відкритих ключів;

передача ідентифікаційних даних фізичних осіб, а також фізичних осіб-представників юридичних осіб (користувачів послуг мобільного зв’язку), які успішно пройшли процес автентифікації за допомогою особистих ключів та сертифікатів відкритих ключів, до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі.

9. Підсистема взаємодії зі схемами електронної ідентифікації з використанням відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, оформленому особі засобами Єдиного державного демографічного реєстру забезпечує виконання таких функцій:

автентифікація інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

автентифікація кваліфікованого надавача електронних довірчих послуг, задіяного у процесах обслуговування сертифікатів відкритих ключів користувачів відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, оформленому особі засобами Єдиного державного демографічного реєстру;

захищений обмін інформацією зі схемами електронної ідентифікації кваліфікованого надавача електронних довірчих послуг;

автентифікація фізичних осіб та фізичних осіб-представників юридичних осіб, які звертаються до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі (користувачів відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, оформленому особі засобами Єдиного державного демографічного реєстру), з використанням особистих ключів та сертифікатів відкритих ключів за запитами від інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

передача ідентифікаційних даних фізичних осіб-представників юридичних осіб (користувачів відображення в електронному вигляді інформації, що міститься у паспорті громадянина України у формі картки, оформленому особі засобами Єдиного державного демографічного реєстру), які успішно пройшли процес автентифікації, до інформаційно-телекомунікаційних систем надання адміністративних та інших видів послуг в електронній формі;

взаємодія із кваліфікованим надавачем електронних довірчих послуг за протоколами визначення статусу сертифікатів відкритих ключів та (додатково) за протоколом управління сертифікатами.

10. Підсистема верифікації відомостей щодо фізичних і юридичних осіб, фізичних осіб - підприємців, які є користувачами системи забезпечує виконання таких функцій:

отримання та передачу відомостей з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань про керівника юридичної особи, керівника її відокремленого підрозділу, інших осіб, які можуть вчиняти дії від імені юридичної особи, керівника громадського формування, що не має статусу юридичної особи, інших осіб, які можуть вчиняти дії від імені громадського формування, що не має статусу юридичної особи, фізичну особу – підприємця, осіб, які можуть вчиняти дії від імені фізичної особи – підприємця (прізвище, ім’я, по батькові (за наявності), дата народження, найменування посади (для керівника), дата призначення або набуття повноважень (для керівника), дата та номер запису в Єдиному державному реєстрі юридичних осіб, фізичних осіб – підприємців та громадських формувань (для фізичної особи – підприємця), реєстраційний номер облікової картки платника податків або серія (за наявності) та номер паспорта громадянина України (для фізичних осіб, які мають відмітку або інформацію в паспорті про право здійснювати платежі за серією та/або номером паспорта), а також про наявність обмежень щодо представництва юридичної особи, громадського формування, що не має статусу юридичної особи, і фізичної особи – підприємця;

верифікацію з використанням інформації Єдиного державного демографічного реєстру засобами єдиної інформаційної системи Міністерства внутрішніх справ України відомостей про прізвище, ім’я та по батькові (за наявності) особи, унікальний номер запису в Єдиному державному демографічному реєстрі, реквізити паспорта громадянина України, паспорта громадянина України для виїзду за кордон, посвідки на постійне проживання та посвідки на тимчасове проживання, оформлених із застосуванням засобів Єдиного державного демографічного реєстру, дійсність зазначених документів;

отримання та передачу відомостей про викрадені (втрачені) документи за зверненнями громадян з єдиної інформаційної системи МВС для встановлення факту втрати або викрадення паспортів громадянина України;

отримання та передачу відомостей з Державного реєстру фізичних осіб - платників податків для підтвердження даних щодо реєстраційного номера облікової картки платника податків або серії (за наявності) та номера паспорта громадянина України (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомили про це відповідний контролюючий орган і мають відмітку у паспорті);

реалізація прикладних програмних інтерфейсів взаємодії підсистеми верифікації відомостей щодо фізичних і юридичних осіб, фізичних осіб - підприємців, які є користувачами системи;

інтеграція з Системою електронної взаємодії державних електронних інформаційних ресурсів;

надання доступу суб’єктам взаємодії до сервісів підсистеми через вебінтерфейс.

11. Підсистема створення та перевірки кваліфікованого електронного підпису забезпечує виконання таких функцій:

робота з особистим ключами;

робота з файловими сховищами сертифікатів та списків відкликаних сертифікатів;

перевірка статусу сертифікатів за протоколом OCSP;

отримання сертифікатів за протоколом CMP;

створення і перевірка удосконаленого електронного підпису;

отримання позначок часу;

інтеграція до зовнішніх вебсайтів у вигляді вебвіджету;

адаптація зовнішнього вигляду вебвіджету під дизайн стороннього вебсайту.

12. Підсистема управління забезпечує виконання технічним адміністратором системи таких функцій:

надання програмних інтерфейсів взаємодії, маркерів (ідентифікаторів) доступу та управління потоками даних між суб’єктами взаємодії системи;

управління технічними ресурсами системи;

управління засобами електроживлення та життєзабезпечення;

реєстрація подій в системі та аварійна сигналізація;

аналіз журналів подій для виконання арбітражних функцій.

13. Підсистема захисту інформації як сукупність технічних та організаційно-технічних рішень повинна відповідати вимогам до комплексної системи захисту інформації (далі – КСЗІ) в інформаційно-телекомунікаційній системі, визначеним законодавством.

14. КСЗІ повинна відповідати вимогам нормативних документів технічного захисту інформації та забезпечувати такі основні функції:

реалізацію політики безпеки інформації заданої для системи;

забезпечення конфіденційності, цілісності, доступності інформації під час її обробки;

розмежування доступу користувачів до захищених ресурсів та сервісів системи, контроль за роботою обслуговуючого персоналу з боку осіб, які відповідають за забезпечення безпеки інформації у системі;

перевірку повноважень користувачів і надання їм права виконання певних дій з обробки захищених ресурсів та використання певних сервісів системи відповідно до визначеної політики безпеки системи;

ідентифікацію та автентифікацію користувачів системи;

реєстрацію подій, пов’язаних із доступом до захищених ресурсів та сервісів системи та дії з ними, результатів ідентифікації та автентифікації користувачів, фактів зміни повноважень користувачів, результатів перевірки цілісності засобів захисту інформації тощо;

блокування несанкціонованих дій щодо захищених ресурсів системи;

захист інформаційних ресурсів та компонентів системи від атак з боку зовнішньої телекомунікаційної мережі та інших мереж з якими система взаємодіє;

захист об’єктів захисту системи під час їх передачі через незахищене середовище;

антивірусний захист системи;

забезпечення цілісності програмного забезпечення системи;

створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації;

керування засобами захисту інформації;

створення умов для забезпечення максимально можливого рівня локалізації негативних наслідків, що завдаються неправомірними та несанкціонованими діями порушників, зменшення негативного впливу наслідків порушення безпеки на функціонування системи;

реєстрація, збір, зберігання, обробка даних про всі події в системі, які мають відношення до безпеки інформації;

забезпечення доступності ресурсів системи для користувачів;

захист інформації від зовнішніх впливів;

інші функції, визначені політикою безпеки системи.

15. Реєстраційні дані (протоколи аудиту) компонентів системи повинні бути захищені від несанкціонованої модифікації та знищення.

16. Комплекси засобів захисту складових частин системи повинні забезпечувати:

конфіденційність та цілісність інформації, яка зберігається й обробляється в компонентах системи, а також передається між ними;

конфіденційність особистих ключів, що використовується у системі, та окремими її користувачами;

конфіденційність технологічної інформації, яка забезпечує функціонування комплексів засобів захисту системи;

доступ до інформації та ресурсів системи користувачам системи згідно з правилами встановленими політикою безпеки (зокрема, правами доступу);

спостережність за діями користувачів шляхом впровадження механізмів і процедур контролю, реєстрації та проведення аудиту зареєстрованих подій.

17. Серверне обладнання та система зберігання даних повинні підтримувати можливість автоматичного резервного копіювання реєстрів користувачів.

18. Зберігання резервних копій повинне здійснюватися у приміщеннях, які територіально відокремлені від приміщень, де розміщено обладнання системи із забезпеченням захисту від несанкціонованого доступу.

19. Порядок резервного копіювання та зберігання резервних копій повинен бути визначений у відповідній інструкції зі складу експлуатаційної документації на систему.

**ІІІ. Організаційні засади діяльності технічного адміністратора системи**

1. Для виконання технічних та технологічних функцій технічний адміністратор системи створює технічний підрозділ, який складається з:

посадової особи, на яку покладено обов’язки керівника технічного підрозділу;

адміністратора реєстрації;

адміністратора безпеки та аудиту;

системного адміністратора.

Для ведення господарської діяльності, пов’язаної із забезпеченням функціонування та розвитком системи, технічний адміністратор системи створює інші відповідні підрозділи та залучає відповідних працівників.

2. Наймані працівники технічного адміністратора системи повинні мати необхідні для надання послуг знання, досвід і кваліфікацію. На посади адміністратора реєстрації, системного адміністратора та адміністратора безпеки та аудиту може бути призначена особа, яка має вищу освіту (ступінь магістра або освітньо-кваліфікаційний рівень спеціаліст), а також стаж роботи у сферах інформаційних технологій, захисту інформації або кібербезпеки не менше двох років. Керівник та наймані працівники повинні бути ознайомлені з положеннями їх посадових інструкцій та діяти відповідно до своїх посадових функцій та завдань.

3. З метою забезпечення захисту інформації в системі шляхом вирішення питань, пов'язаних з проектуванням, розробленням, модернізацією, введенням в експлуатацію та підтримкою працездатності КСЗІ та додержання режиму безпеки в системі створюється підрозділ служби захисту інформації (далі – СЗІ).

До складу СЗІ входять:

посадова особа, на яку покладено обов'язки керівника СЗІ;

адміністратор безпеки та аудиту;

системний адміністратор;

адміністратор реєстрації.

Основними функціями СЗІ є:

забезпечення повноти та якісного виконання організаційно-технічних заходів із захисту інформації;

розроблення розпорядчих документів, згідно з якими технічний адміністратор системи повинен забезпечувати захист інформації, контроль за їх виконанням;

своєчасне реагування на спроби несанкціонованого доступу до інформаційних ресурсів системи, порушення правил експлуатації засобів захисту інформації.

Обов'язки керівника СЗІ покладаються на посадову особу, на яку покладено обов'язки керівника технічного підрозділу.

Керівник СЗІ забезпечує належне виконання СЗІ її функцій.

4. Адміністратор реєстрації відповідає за укладання договорів про приєднання до інтегрованої системи електронної ідентифікації (далі – Договір про приєднання) та за безпосереднє приєднання інформаційно-телекомунікаційних систем суб’єктів взаємодії до системи.

Основними обов'язками адміністратора реєстрації є:

ідентифікація та автентифікація суб’єктів взаємодії, які звернулися до технічного адміністратора системи із Договором про приєднання;

узгодження проєктів Договорів про приєднання;

здійснення приєднання інформаційно-телекомунікаційних систем суб’єктів взаємодії до системи;

ведення обліку суб’єктів та об’єктів взаємодії, приєднаних до системи;

надання консультацій щодо умов та порядку приєднання інформаційно-телекомунікаційних систем суб’єктів взаємодії до системи.

5. Адміністратор безпеки та аудиту відповідає за належне функціонування КСЗІ та здійснення перевірок дотримання найманими працівниками вимог внутрішньої організаційно-розпорядчої документації та документації на КСЗІ.

Основними обов’язками адміністратора безпеки та аудиту є:

організація розмежування доступу до ресурсів системи;

спостереження за функціонуванням КСЗІ (реєстрація подій в системі, моніторинг подій тощо);

організація та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій системи;

забезпечення режиму доступу до приміщень, в яких розміщено технічні засоби системи;

ведення журналів обліку адміністратора безпеки та аудиту, передбачених документацією на КСЗІ;

здійснення перевірок журналів аудиту подій, що реєструють технічні засоби системи;

здійснення перевірок відповідності внутрішньої організаційно-розпорядчої документації технічного адміністратора системи та документації на КСЗІ;

контроль за дотриманням найманими працівниками внутрішньої організаційно-розпорядчої документації технічного адміністратора системи та документації на КСЗІ.

6. Системний адміністратор відповідає за функціонування програмно-апаратних комплексів держателя та технічного адміністратора системи і технічних засобів системи.

Основними обов'язками системного адміністратора є:

організація експлуатації та технічного обслуговування системи і адміністрування її технічних засобів;

забезпечення функціонування вебсайту системи;

участь у впровадженні та забезпеченні функціонування КСЗІ;

налаштування ведення журналів аудиту подій, що реєструють технічні засоби системи;

встановлення, налаштування та забезпечення підтримки працездатності загальносистемного та спеціального програмного забезпечення системи;

встановлення та налагодження штатної підсистеми резервного копіювання даних системи;

забезпечення актуалізації даних, створюваних та оброблюваних в системі, після збоїв.

**IV. Вимоги щодо ідентифікації та автентифікації суб’єктів взаємодії та порядок приєднання інформаційно-телекомунікаційних систем суб’єктів взаємодії до системи.**

1. Приєднання інформаційно-телекомунікаційних систем суб’єктів взаємодії до системи здійснюється на підставі Примірного Договору про приєднання. Форму Договору про приєднання розміщено на вебсайті системи ([https://id.gov.ua](https://id.gov.ua/)).

2. Технічний адміністратор системи в особі адміністратора реєстрації здійснює ідентифікацію, автентифікацію та перевірку достатності обсягу цивільної правоздатності та дієздатності суб’єкта взаємодії.

3. Перевірка обсягу повноважень уповноваженого представника юридичної особи або фізичної особи – підприємця здійснюється за документом або за даними з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань, що визначають повноваження представника.

4. Перевірка обсягу повноважень уповноваженого представника колегіального органу юридичної особи здійснюється за документом, у якому визначено повноваження відповідного органу та розподіл обов'язків між його членами.

5. Ідентифікація іноземців та осіб без громадянства здійснюється відповідно до законодавства.

6. Після укладання Договору про приєднання адміністратор реєстрації разом з відповідальною особою суб’єкта взаємодії встановлює ідентифікатори доступу інформаційно-телекомунікаційної системи суб’єкта взаємодії, визначені протоколом OAuth 2.0:

ідентифікатор прикладної системи client\_id, який однозначно ідентифікує інформаційно-телекомунікаційну систему суб’єкта взаємодії;

секретний рядок доступу client\_secret, за якою система видаватиме інформаційно-телекомунікаційній системі суб’єкта взаємодії маркер доступу access\_token;

кваліфікований сертифікат електронної печатки з відміткою про призначення відкритого ключа для протоколу розподілу ключів направленого шифрування інформації про користувача системи під час її передачі між системою та інформаційно-телекомунікаційною системою суб’єкта взаємодії.

7. Після встановлення ідентифікаторів доступу інформаційно-телекомунікаційної системи суб’єкта взаємодії технічний адміністратор системи здійснює передачу суб’єкту взаємодії ідентифікаторів доступу у зашифрованому вигляді, приклади використання ресурсів системи та бібліотеки підпису, шляхом направлення електронного листа на електронну адресу відповідальної особи суб’єкта взаємодії, вказану у Договорі про приєднання. Шифрування здійснюється з використанням особистого ключа, відповідний якому відкритий ключ внесено до кваліфікованого сертифіката електронної печатки технічного адміністратора системи, призначеної для здійснення інформаційного обміну з суб’єктами взаємодії, та кваліфікованого сертифіката відповідальної особи суб’єкта взаємодії/кваліфікованого сертифіката електронної печатки суб’єкта взаємодії.

8. Технічний адміністратор має право заблокувати доступ інформаційно-телекомунікаційної системи суб’єкта взаємодії до системи у разі:

надходження інформації про можливий несанкціонований доступ до ідентифікаторів доступу інформаційно-телекомунікаційної системи;

виникнення підозри щодо здійснення вірусних атак в інформаційно-телекомунікаційній системі суб’єкта взаємодії (до повного усунення загрози);

виникнення обставин, визначених у Договорі про приєднання.

**V. Вимоги щодо надання послуг транскордонної електронної ідентифікації**

1. Визнання засобів та схем електронної ідентифікації, що використовуються під час надання послуг транскордонної електронної ідентифікації у процесі взаємодії між суб’єктами різних держав забезпечується шляхом укладення відповідного міжнародного договору України про взаємне визнання засобів та схем електронної ідентифікації (далі – міжнародний договір).

2. Процедури захищеного обміну та управління інформаційними потоками під час транскордонної електронної ідентифікації описуються у форматах, протоколах, алгоритмах та об’єктних ідентифікаторах, які використовуються у засобах електронної ідентифікації під час надання послуг з транскордонної електронної ідентифікації, та виконуються відповідно до умов міжнародного договору.

**Директор директорату**

**функціонального розвитку цифровізації Анастасія ХАЛЄЄВА**