

24600348.01.П-ЗК

Прим. № _____

ЗАТВЕРДЖУЮ

Директор ТОВ «ДІО – ТРЕЙДЕР ІНТЕРНАЦІОНАЛ»

М.Г. Кращенко

« 05 » / 06 2026 р.

ПОРЯДОК

**взаємодії інформаційно-комунікаційної системи «Система захищеного
доступу до державних електронних реєстрів» із зовнішніми
користувачами**

24600348.01.П-ЗК

Версія 1.0

м. Кривий Ріг

2026 рік

АРКУШ РЕЄСТРАЦІЇ ДОКУМЕНТА

Реквізит	Значення
Повна назва	Порядок взаємодії інформаційно-комунікаційної системи «Система захищеного доступу до державних електронних реєстрів» із зовнішніми користувачами
Шифр документа	24600348.01.П-ЗК
Власник системи	ТОВ «Д.І.О. – ТРЕЙДЕР ІНТЕРНАЦІОНАЛ» (ЄДРПОУ 24600348)
Покриває заходи ЦПБ	АС-20, АС-20(1), АС-20(2)
Категорія БПБ	БПБ системи, де обробляється відкрита або конфіденційна інформація (Наказ Адміністрації Держспецзв'язку від 30.06.2025 № 409)
Версія / Дата	1.0 / 2026 р.
Статус	Чинний. Надається зовнішнім користувачам
Розробник	Керівник підрозділу із кіберзахисту ІКС «СЗД ДЕР»
Затверджує	Директор ТОВ «Д.І.О. – ТРЕЙДЕР ІНТЕРНАЦІОНАЛ»
Періодичність перегляду	Щонайменше щороку та за визначеними тригерами

Історія змін

Версія	Дата	Автор	Зміст змін
1.0	2026	Керівник підрозділу із кіберзахисту	Першу редакцію розроблено на заміну порядку створення КСЗІ на типових робочих місцях зовнішніх користувачів (24600348.152.M1 01-01)

ПЕРЕЛІК СКОРОЧЕНЬ, ТЕРМІНІВ ТА ВИЗНАЧЕНЬ

Скорочення / термін	Визначення
ІКС «СЗД ДЕР», ІКС, система	Інформаційно-комунікаційна система «Система захищеного доступу до державних електронних реєстрів», власник – ТОВ «Д.І.О. – ТРЕЙДЕР ІНТЕРНАЦІОНАЛ»
Порядок	Порядок взаємодії інформаційно-комунікаційної системи «Система захищеного доступу до державних електронних реєстрів» із зовнішніми користувачами (24600348.01.П-ЗК)
ТОВ	ТОВ «Д.І.О. – ТРЕЙДЕР ІНТЕРНАЦІОНАЛ» (ЄДРПОУ 24600348) – власник та адміністратор ІКС «СЗД ДЕР»
Зовнішній користувач, користувач	Суб'єкт господарювання / філія суб'єкта господарювання, працівники якого отримують право взаємодії з ІКС «СЗД ДЕР» на умовах цього Порядку
Оператор	Уповноважена особа зовнішнього користувача, яка використовує РС для роботи з прикладним ПЗ ІКС «СЗД ДЕР» у межах наданих повноважень
Робоче місце, РМ	Сукупність апаратно-програмних (технічних) засобів та контрольованого фізичного середовища, призначених для обробки інформації та взаємодії з ІКС «СЗД ДЕР»
Робоча станція, РС	Робоча станція – технічний засіб РМ, на базі якого здійснюється доступ до прикладного ПЗ ІКС «СЗД ДЕР»
Мобільна РС	Робоча станція переносного типу (ноутбук, нетбук)
ОС	Операційна система робочої станції
ЦПБ	Цільовий профіль безпеки ІКС «СЗД ДЕР»
СЗІ	Система захисту інформації ІКС «СЗД ДЕР»
ТЗІ / КЗІ	Технічний / криптографічний захист інформації
ПК КЗІ	Програмний комплекс криптографічного захисту інформації «ІТ Захист з'єднань-2. Клієнт захисту з'єднань»
НКІ	Носій ключової інформації (електронний ключ «Кристал-1», «Алмаз-1К» або інший сумісний з архітектурою ІКС «СЗД ДЕР» засіб з чинним експертним висновком у сфері КЗІ)
КЕП	Кваліфікований електронний підпис
КНЕДП	Кваліфікований надавач електронних довірчих послуг
ЕВ	Експертний висновок за результатами державної експертизи у відповідній сфері (ТЗІ або КЗІ)
Обліковий запис	Унікальний запис в ОС РС, що використовується для ідентифікації оператора та надання відповідного рівня доступу
Адміністративний обліковий запис	Обліковий запис ОС із розширеними повноваженнями для адміністрування та технічного обслуговування РС

Скорочення / термін	Визначення
Критичні оновлення	Оновлення ПЗ, що усувають уразливості або помилки, які можуть істотно вплинути на безпеку чи стабільність роботи
Білий список носіїв	Визначений перелік дозволених змінних носіїв, використання яких допускається на РС
Формуляр на РС	Документ облікового характеру з відомостями про склад РС, встановлене ПЗ, його версії та апаратні характеристики
Акт перевірки, Акт	Акт перевірки відповідності робочого місця та акцепту вимог Порядку щодо захисту інформації на робочих місцях, що взаємодіють з ІКС «Система захищеного доступу до державних електронних реєстрів» (Додаток А)

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Призначення

Цей Порядок є угодою безпеки взаємозв'язку з ІКС «СЗД ДЕР» та встановлює уніфіковані вимоги щодо використання прикладного ПЗ підсистеми ІКС згідно з його цільовим призначенням, відповідності діяльності зовнішнього користувача видам діяльності, задля яких надається доступ до прикладного ПЗ підсистеми ІКС, дотримання користувачами нормативних документів та інструкцій (настанов) щодо роботи з прикладним ПЗ підсистеми ІКС та вимог щодо захисту інформації при взаємодії з ІКС, в тому числі вимоги до забезпечення захисту робочих місць зовнішніх користувачів (операторів), що підключаються до ІКС «СЗД ДЕР» для захищеної взаємодії з державними електронними реєстрами (зокрема, ЄДР ТЗ, НАІС ГСЦ МВС, ЄДР МВС).

Вимоги Порядку реалізують заходи захисту АС-20 «Використання зовнішніх систем», АС-20(1) «Обмеження на авторизоване використання» та АС-20(2) «Переносні пристрої зберігання даних» Цільового профілю безпеки ІКС «СЗД ДЕР» у частині зовнішніх систем (РМ зовнішніх користувачів), з яких здійснюється доступ до системи.

З набрання чинності цього Порядку, підключення РМ зовнішніх користувачів здійснюється без створення окремих комплексних систем захисту інформації (КСЗІ) на типових робочих місцях. Інструкція про порядок розгортання, введення та виведення з експлуатації типового робочого місця зовнішнього користувача (24600348.152.М1 01-01) та комплект шаблонів документів КСЗІ «Клієнт-СД» застосовуються лише до РМ, підключених до набрання чинності цього Порядку, до моменту подання такими користувачами першого Акта перевірки за Додатком А.

1.2. Нормативні підстави

- Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
- Постанова Кабінету Міністрів України від 18.06.2025 № 712 «Порядок авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем»;
- Постанова Кабінету Міністрів України від 29.03.2026 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем»;

- Наказ Адміністрації Держспецв'язку від 30.06.2025 № 409 «Про затвердження базового профілю безпеки системи, де обробляється відкрита або конфіденційна інформація»;
- Цільовий профіль безпеки ІКС «СЗД ДЕР»;
- Політика керування доступом 24600348.01.П-АС та Процедура керування доступом 24600348.01.ПР-АС;

1.3. Покриття вимог ЦПБ

Відповідність розділів цих Вимог заходам захисту ЦПБ наведено в таблиці 1.1.

Таблиця 1.1 – Покриття заходів ЦПБ

Захід ЦПБ	Зміст заходу	Розділи цих Вимог
АС-20.1	Встановлення умов взаємодії та визначення технічних і організаційних засобів контролю на зовнішніх системах, що дозволяють уповноваженим особам доступ до системи із зовнішніх систем	пп. 1.4, 1.6 розділи 2, 3
АС-20.2	Заборона використання особистих мобільних пристроїв співробітників (BYOD) та публічних комп'ютерів	п. 2.3
АС-20(1)	Дозвіл на використання зовнішньої системи лише після перевірки виконання заходів безпеки та за наявності збережених угод про підключення	розділ 4
АС-20(2)	Обмеження використання переносних пристроїв зберігання даних на зовнішніх системах: заборона незатверджених носіїв, обов'язковий антивірусний контроль перед використанням	п. 3.6

1.4. Умови підключення (надання доступу) та взаємодії

Доступ користувачів до прикладного ПЗ ІКС «СЗД ДЕР» надається за наступних умов:

- використання прикладного ПЗ системи згідно з його цільовим призначенням;
- відповідність діяльності користувача видам діяльності, задля яких надається доступ до прикладного ПЗ системи;
- дотримання користувачами та операторами нормативних документів та інструкцій (настанов) щодо роботи з прикладним ПЗ системи;
- виконання вимог цього Порядку щодо захисту інформації.

1.5. Облік робочих станцій

ТОВ «Д.І.О. – ТРЕЙДЕР ІНТЕРНАЦІОНАЛ» з метою збору ідентифікаційних даних здійснює облік робочих місць з робочими станціями та користувачів разом з операторами, що взаємодіють із системою. Облік дозволяє своєчасно отримувати інформацію про можливі порушення політики безпеки та полегшує розслідування інцидентів безпеки.

Обліку підлягають такі дані

1. Про користувача, РМ та його операторів:

- Повна та скорочена назва користувача;
- Код за ЄДРПОУ/ІПН;
- Номер у відповідному державному реєстрі для суб'єктів проведення визначеної діяльності;
- Адреса (юридична та робочого місця);
- ПІБ, контакти керівника підрозділу/філії користувача, в якому розгорнуто РМ;
- ПІБ, контакти уповноважених осіб яким планується надати доступ до прикладного ПЗ ІКС.

2. Про робочі станції:

- Номер приміщення РМ, в якому розташована РС;
- інвентарний номер РС;
- операційна система;
- встановлений антивірусний засіб (із зазначенням реквізитів ЕВ у сфері ТЗІ);
- встановлений ПК КЗІ (із зазначенням реквізитів ЕВ у сфері КЗІ);
- назва та серійний/заводський номер НКІ.
- веб-браузер для доступу до прикладного ПЗ ІКС «СЗД ДЕР»
- допоміжне функціональне ПЗ РС для роботи з прикладним ПЗ ІКС «СЗД ДЕР»

У разі наявності мобільних РС додатково вказуються: марка, модель, серійний номер РС, визначене місце зберігання РС та застосований засіб повнодискового шифрування.

Надання ідентифікаційних даних здійснюється за формою Акта (таблиці 1, 2 Додатка А).

1.6. Обов'язки та відповідальність

Керівництвом користувача має бути визначено відповідальну(-их) особу(осіб) за захист інформації на РМ (на яку (яких) покладаються обов'язки із забезпечення виконання вимог розділів 2, 3 цього Порядку та періодичного контролю за їх дотриманням) та особу (осіб), що забезпечує(-ють) адміністрування, технічне обслуговування РС.

Дозволяється покладати на одну особу обов'язки відповідального за захист інформації на РМ та обов'язки відповідального за адміністрування, технічне обслуговування РС.

Дозволяється покладати на одну особу обов'язки відповідального за захист інформації кількох РМ у межах зовнішнього користувача.

Для розгортання та перевірки РМ створюється Робоча група у складі відповідального за адміністрування та технічне обслуговування РС і відповідального за захист інформації РМ.

Керівництво користувача несе відповідальність за реалізацію заходів захисту на РМ та зобов'язане оперативно (не пізніше строків, визначених п. 3.9) повідомляти ТОВ про зміну персоналу (операторів), який має доступ до прикладного ПЗ системи.

1.7. Звітність і термін дії дозволу

Ідентифікаційні дані РМ, РС, користувачів та їх операторів та результати перевірки виконання вимог розділів 2, 3 оформляються Актом за формою Додатка А, що затверджується керівництвом користувача та скан-копія якого надсилається ТОВ.

Керівництвом користувача кожні 2 роки затверджується оновлений (плановий) Акт перевірки, скан-копія якого одразу подається до ТОВ.

Цей Порядок підлягає щорічному перегляду ТОВ на предмет актуальності діючих вимог щодо захисту інформації, за результатами якого можуть вноситись зміни, про які повідомляється зовнішньому користувачу.

Якщо вищевказані зміни впливають на вимоги щодо захисту інформації на РМ користувача, то користувач зобов'язаний провести відповідні оновлення засобів захисту РМ та скласти Акт позапланової перевірки, скан-копію якого надіслати ТОВ.

2. ВИМОГИ ДО РОБОЧИХ МІСЦЬ

2.1. Вимоги до апаратного забезпечення

Перелік та характеристики апаратного забезпечення РС визначаються технічною документацією щодо роботи з прикладним ПЗ ІКС, а саме “Настановами для користувача”, що надається ТОВ.

Робоча станція, з якої здійснюється доступ до прикладного ПЗ ІКС «СЗД ДЕР», має перебувати на внутрішньому обліку користувача та мати унікальний інвентарний номер.

На РМ має бути наявний НКІ, призначений для зберігання особистих ключів користувача: електронний ключ «Кристал-1», «Алмаз-1К» або інший сумісний з архітектурою ІКС «СЗД ДЕР» засіб, що має чинний ЕВ у сфері КЗІ. НКІ має відповідати вимогам експлуатаційної документації.

Мережеве обладнання має забезпечувати підключення РС до мережі Інтернет з пропускнуою здатністю не менше ніж 1 Mbit/s.

2.2. Вимоги до складу програмного забезпечення

На РС встановлюються виключно:

- операційна система, що перебуває на підтримці виробника та отримує оновлення безпеки;
- веб-браузер(и), що підтримує(ють) взаємодію з прикладним ПЗ системи: Mozilla Firefox або Google Chrome останньої версії;
- ПК КЗІ «ІТ Захист з'єднань-2. Клієнт захисту з'єднань», що має чинний ЕВ у сфері КЗІ, – для захисту каналу зв'язку із системою;
- засоби формування та перевірки КЕП, сумісні з КНЕДП, що обслуговує систему (web-бібліотеки підпису (агент підпису) зі складу Програмного комплексу користувача ЦСК "ІТ Користувач ЦСК-1");
- засіб антивірусного захисту, що має чинний позитивний ЕВ у сфері ТЗІ;
- за необхідності, допоміжне програмне забезпечення функціонального призначення:
 - Java версії 8 та вище;
 - MS Office, LibreOffice, FreeOffice, Adobe Acrobat Reader, Sumatra PDF із налаштуванням заборони виконання макросів.

Встановлення будь-якого іншого програмного забезпечення, окрім зазначеного в даному Порядку, забороняється. Склад та версії встановленого ПЗ фіксуються у Формулярі на РС (п. 3.7).

2.3. Заборона використання неавторизованих систем

Відповідно до заходу АС-20.2 ЦПБ для доступу до ІКС «СЗД ДЕР» забороняється використання:

- особистих мобільних пристроїв та особистих комп'ютерів співробітників (BYOD);
- робота з публічних та спільних комп'ютерів (інтернет-кафе, бібліотеки, готелі тощо);
- будь-яких інших робочих станцій, не зазначених у чинному Акті.

2.4. Вимоги до приміщень

На приміщення, в якому розгорнуте РМ, мають поширюватися правила перепускного режиму із виконанням заходів фізичної безпеки, визначених п. 3.10.

Приміщення має бути обладнано сейфом або робочою шафою, обладнаною замком та засобом для опечатування (опломбування), для зберігання НКІ та облікової документації.

3. ВИМОГИ ДО БЕЗПЕЧНОЇ ОБРОБКИ ІНФОРМАЦІЇ НА РОБОЧОМУ МІСЦІ

3.1. Управління обліковими записами ОС РС

3.1.1. Політикою налаштування ОС має бути забезпечено:

- відокремлення повноважень оператора та адміністратора;
- мінімізацію повноважень оператора;
- блокування гостьових, вбудованих, анонімних облікових записів та обмеження інтерактивного входу в ОС для наявних облікових записів.

Доступ до адміністративного облікового запису ОС надається лише особі або підрозділу, що забезпечує адміністрування та технічне обслуговування РС.

Має вестися реєстр (відомість) облікових записів ОС із зазначенням власника облікового запису ОС та записами періодичного контролю.

3.1.2. Облікові записи ОС підлягають щоквартальному контролю.

3.1.3. Оператор зобов'язаний завершувати роботу на РС наприкінці робочого дня.

3.2. Забезпечення цілісності інформації

3.2.1. Робочі станції мають передбачати захист від несанкціонованого завантаження сторонніх ОС (пароль на BIOS/UEFI, заборона завантаження зі змінних носіїв), за допомогою яких можуть бути внесені зміни у файлову систему або порушена цілісність основної ОС.

3.2.2. Робоча станція має бути опломбована таким чином, щоб виключити доступ до внутрішніх компонентів. У разі технічного обслуговування акт пломбування РС оновлюється.

3.2.3. Антивірусне ПЗ має забезпечувати сканування файлів у реальному часі та сканування змінних носіїв, що підключаються до РС. Налаштування мають забезпечувати щонайменше середній рівень безпеки за критеріями виробника та щотижневу повну перевірку ОС на наявність шкідливого ПЗ.

3.2.4. На РС має використовуватися актуальне ПЗ – ОС, веб-браузер, антивірусний засіб. Критичні оновлення мають встановлюватися у строк до 30 днів.

3.2.5. Політикою ОС має бути встановлене автоматичне блокування облікового запису після 30 хвилин бездіяльності. Розблокування ОС здійснюється виключно шляхом повторної автентифікації оператора.

3.2.6. Екран блокування має приховувати вміст ОС. Функції адаптивного блокування екрана (розблокування за наявності Bluetooth-пристрою та інші тригерні події) мають бути вимкнені.

3.3. Політика використання паролів

3.3.1. Політикою ОС має бути встановлено мінімальну довжину пароля облікового запису 12 символів та вимоги до складності (цифри, літери верхнього і нижнього регістру, спеціальні символи), а також зміну пароля кожні 180 днів. Відновлення або примусова зміна пароля облікового запису оператора ОС здійснюється з адміністративного облікового запису ОС.

3.3.2. Оператори мають бути поінформовані про неприпустимість використання однакових паролів: новий пароль має відрізнятися від попереднього щонайменше на 50 % символів.

3.4. Забезпечення захисту РС та мережевого захисту

3.4.1. Доступ до прикладного ПЗ ІКС «СЗД ДЕР» здійснюється виключно через програмний шлюз захисту ТОВ із криптографічним захистом каналу зв'язку засобами ПК КЗІ «ІТ Захист з'єднань-2». Передача електронного документа до державного реєстру здійснюється разом із завершенням його створення шляхом накладення на нього КЕП.

3.4.2. Сеанс ПК КЗІ має завершуватися одразу після закінчення роботи з прикладним ПЗ ІКС. НКІ підключається до РС лише на час сеансу та зберігається у сейфі (шафі) відповідно до п. 2.4.

3.4.3. Мобільні РС підлягають обов'язковому повнодисковому шифруванню.

3.4.4. Оператору заборонено використовувати РС для власних потреб та/або завдань, які не передбачають обробку даних в прикладному ПЗ ІКС «СЗД ДЕР».

3.4.5. У налаштуваннях браузера мають бути заборонені автозаповнення форм, збереження паролів та синхронізація паролів з хмарними сервісами, ввімкнено автоматичне видалення тимчасових файлів сайтів (cookie та кеш) при виході з браузера та функції ізоляції сайтів. Браузер не повинен містити плагінів та розширень, що не є необхідними для роботи з прикладним ПЗ ІКС.

3.4.6. Тимчасові файли, що утворюються під час роботи, мають видалятися з РС без можливості відновлення після закінчення роботи з ними.

3.5. Журнали аудиту

Політикою налаштування ОС має бути забезпечено реєстрацію подій входу та виходу операторів (у тому числі від імені адміністративного облікового запису ОС). Функції перегляду та очищення журналів подій мають бути доступні лише адміністративному обліковому запису ОС.

3.6. Управління носіями

3.6.1. Використання переносних пристроїв зберігання даних на РМ обмежується відповідно до заходу АС-20(2) ЦПБ: використання незатверджених носіїв заборонено, кожен носій підлягає обов'язковому антивірусному контролю перед використанням.

3.6.2. Усі змінні носії інформації мають бути обліковані та внесені до реєстру (відомості) носіїв із зазначенням ідентифікатора та власника носія. Реєстр зберігається у надійному місці. НКІ обліковуються окремо.

3.6.3. На РС засобами ОС має бути налаштовано «білий список» дозволених носіїв згідно з реєстром. Автозапуск будь-яких змінних носіїв має бути відключений.

3.6.4. Усі надані ТОВ паперові носії інформації (інструкції, договори тощо) мають зберігатися у надійному місці.

3.7. Управління конфігурацією

3.7.1. Усі конфігурації мають документуватися та періодично переглядатися. Обов'язковому документуванню підлягають: параметри локальних політик безпеки ОС, параметри конфігурації мережевого обладнання, що комутує трафік між РС та програмним шлюзом захисту ТОВ, параметри конфігурацій ПК КЗІ та засобів доступу до мережі.

3.7.2. Має вестися Формуляр на РС із переліком та версіями встановленого ПЗ і відомостями щодо апаратного складу.

3.8. Реагування на інциденти

3.8.1. Користувачем має бути розроблена Інструкція з реагування на інциденти інформаційної безпеки, яка містить: відповідальних за реагування на робочому місці, канали комунікацій про інциденти (включно з контактами ТОВ), типи можливих інцидентів, процедури дій у разі втрати мобільної РС та/або НКІ, відповідальність користувача/оператора за недотримання порядку реагування.

3.8.2. Про інциденти, пов'язані із взаємодією з ІКС «СЗД ДЕР» (компрометація облікових даних або особистих ключів, втрата НКІ чи мобільної РС, виявлення шкідливого ПЗ, ознаки несанкціонованого доступу), оператор невідкладно, але не пізніше 24 годин з моменту виявлення, повідомляє ТОВ визначеними каналами зв'язку. У разі

компрометації особистих ключів користувач невідкладно ініціює скасування відповідних сертифікатів.

3.8.3. Зовнішнім користувачем має бути забезпечено навчання операторів щодо порядку реагування на інциденти до моменту отримання доступу до прикладного ПЗ ІКС та щороку після цього. Оператори ознайомлюються з Інструкцією під підпис.

3.9. Скасування доступу та зміна персоналу

3.9.1. У разі зміни функціональних обов'язків оператора, що не передбачає обробку інформації в прикладному ПЗ ІКС, відповідальна особа користувача інформує ТОВ про скасування доступу такому оператору протягом 3 робочих днів. Рекомендується завчасне інформування із зазначенням дати скасування доступу.

3.9.2. У разі добровільного припинення трудових відносин користувача із оператором, користувач інформує про це ТОВ протягом 3 робочих днів.

3.9.3. У разі примусового припинення трудових відносин користувача із оператором, користувач інформує про це ТОВ негайно.

3.9.4. Одночасно з повідомленням про припинення трудових відносин користувача з оператором, користувач забезпечує вилучення НКІ у оператора та, за потреби, ініціює скасування сертифікатів відкритих ключів.

3.10. Фізична безпека

3.10.1. На приміщення, в якому розгорнуто РМ (та зберігається мобільна РС, за наявності такої), мають поширюватися правила перепускного режиму, затверджені керівництвом користувача.

3.10.2. У неробочий час приміщення має бути забезпечено охоронною сигналізацією та/або охороною та/або засобом для опечатування (опломбування).

4. ПОРЯДОК ПІДКЛЮЧЕННЯ ТА КОНТРОЛЬ ВИКОНАННЯ ВИМОГ

4.1. Надання доступу

Відповідно до заходу АС-20(1) ЦПБ доступ уповноважених осіб користувача до прикладного ПЗ ІКС з РМ надається лише після:

- виконання вимог цього Порядку;
- подання користувачем скан-копії затвердженого Акту перевірки (Додаток А) з ідентифікаційними даними РМ, РС, користувача та операторів;
- перевірки ТОВ виконання заходів безпеки, зазначених в Акті (документальна перевірка, за рішенням ТОВ – додаткова вибіркова перевірка);
- реєстрації користувача та операторів в Реєстрі зовнішніх систем ТОВ і видачі облікових даних користувачу.

4.2. Збереження угод

ТОВ зберігає укладені з користувачами договори, Акти та пов'язані документи протягом усього строку дії підключення та щонайменше 2 років після його припинення. Облік підключень веде Адміністратор ПЗ ТОВ.

4.3. Контроль та призупинення доступу

ТОВ має право здійснювати вибіркові перевірки дотримання вимог цього Порядку, у тому числі запитувати підтвердні документи та проводити дистанційні перевірки конфігурацій у погоджений з користувачем час.

Доступ до прикладного ПЗ ІКС призупиняється у разі незабезпечення виконання користувачем вимог щодо засобів та заходів, направлених на захист інформації, зазначених у цьому Порядку, зокрема:

- неподання оновленого Акта у строк, визначений п. 1.7;
- виявлення невиконання вимог розділів 2, 3
- виявлення інциденту безпеки, пов'язаного з РМ користувача, – до завершення розслідування та усунення причин.

Поновлення доступу здійснюється після усунення виявлених невідповідностей та подання оновленого Акта.

4.4. Відповідальність

4.4.1 Порушення вимог цього Порядку, що призвело або могло призвести до порушення конфіденційності, цілісності чи доступності інформації в ІКС «СЗД ДЕР», є підставою для призупинення або припинення доступу до прикладного ПЗ ІКС.

4.4.2 Користувач повинен забезпечувати дотримання при правовідносинах вимог Закону України «Про захист персональних даних», шляхом підписання усіх необхідних документів. Користувач засвідчує та гарантує, що будь-які персональні дані про будь-яких фізичних осіб, які були або будуть передані ТОВ та ІКС, були отримані та знаходяться у користуванні користувача правомірно відповідно до вимог чинного законодавства України. Користувач засвідчує і гарантує, що він має всі необхідні правові підстави для передачі вищевказаних персональних даних ТОВ та ІКС для їх подальшої обробки з метою виконання зобов'язань, без будь-якого обмеження строком та способом, у т.ч. для їх використання, поширення, зміни, передачі чи надання доступу до них третім особам у випадках, передбачених чинним законодавством України, а також для передачі персональних даних для обробки третім особам та здійснення відносно них будь-яких інших дій, якщо це пов'язано із виконанням зобов'язань та/або із захистом прав ТОВ, або якщо це необхідно для реалізації прав та обов'язків, передбачених Законом. Право користувача на передачу вищевказаних персональних даних нічим не обмежене і не порушує права суб'єктів персональних даних та інших осіб.

4.4.3 Порушення зобов'язань викладених в пункті 4.4.2 цього Порядку також є підставою для призупинення або припинення доступу до прикладного ПЗ ІКС.

ДОДАТОК А

до Порядку 24600348.01.П-ЗК

ЗАТВЕРДЖУЮ

Керівник _____

(найменування зовнішнього користувача)

(ПРИЗВИЩЕ Ім'я керівника)_____
(підпис)

« ____ » _____ 20 ____ року

АКТ № _____

перевірки відповідності робочого місця та акцепту вимог Порядку щодо захисту інформації на робочих місцях, що взаємодіють з ІКС «Система захищеного доступу до державних електронних реєстрів»

Вид перевірки: первинна / планова / позапланова (потрібне підкреслити).

Робочою групою з боку _____ (найменування зовнішнього користувача) проведено перевірку робочого місця на відповідність вимогам Порядку 24600348.01.П-ЗК.

Склад робочої групи:

відповідальний за захист інформації (ПІБ, e-mail, номер моб. телефону):

відповідальний за адміністрування та технічне обслуговування РС (ПІБ):

Під час перевірки встановлено таке:

Таблиця 1 – Ідентифікаційні дані користувача, робочого місця (РМ) та його операторів

Найменування	Відомості
Повна назва зовнішнього користувача	
Скорочена назва зовнішнього користувача	
Код за ЄДРПОУ/ПІН	
Номер у відповідному державному реєстрі для суб'єктів проведення визначеної діяльності	

Найменування	Відомості
Юридична адреса	
Адреса робочого місця (РМ)	
ПІБ, контакти керівника підрозділу/філії користувача, в якому розгорнуто РМ	
ПІБ, контакти уповноважених осіб (операторів), яким планується надати доступ до прикладного ПЗ «СЗД ДЕР»	

Таблиця 2 – Ідентифікаційні дані робочої станції (РС)

Найменування	Відомості
Тип РС (стаціонарна/мобільна)	
№ приміщення РМ, де розташована РС	
Інвентарний номер РС	
Місце зберігання мобільної РС (адреса, № приміщення) (тільки для мобільної РС)	
Марка, модель, серійний номер РС (тільки для мобільної РС)	
Операційна система (назва, версія)	
Антивірусний засіб (назва, версія та реквізити ЕВ ТЗІ)	
ПК КЗІ та реквізити ЕВ КЗІ	
Назва та серійний/заводський номер НКІ	
Веб-браузер для доступу до прикладного ПЗ ІКС «СЗД ДЕР»	
Засіб формування та перевірки КЕПІ	
Допоміжне функціональне ПЗ РС для роботи з прикладним ПЗ ІКС «СЗД ДЕР» (назви)	
Засіб повнодискового шифрування (тільки для мобільної РС)	

Таблиця 3 – Відомості щодо виконання вимог

Розділ Порядку	Виконано (Так/Ні)	Примітки (за необхідності)
2.1. Апаратне забезпечення		
2.2. Склад програмного забезпечення		
2.3. Заборона неавторизованих систем (BYOD, публічні комп'ютери)		

Розділ Порядку	Виконано (Так/Ні)	Примітки (за необхідності)
2.4. Вимоги до приміщень		
3.1. Управління обліковими записами		
3.2. Забезпечення цілісності інформації		
3.3. Політика використання паролів		
3.4. Захист РС та мережевий захист		
3.5. Журнали аудиту		
3.6. Управління носіями		
3.7. Управління конфігурацією		
3.8. Реагування на інциденти		
3.9. Скасування доступу та зміна персоналу		
3.10. Фізична безпека		

Висновки

Робоча група підтверджує, що в повному обсязі виконано встановлені вимоги та заходи захисту інформації, передбачені вимогами Порядку 24600348.01.П-ЗК.

Оператори ознайомлені з відповідними інструкціями під підпис, усвідомлюють пов'язані ризики (у тому числі ризики несанкціонованого доступу, втрати або компрометації інформації у разі порушення вимог) і беруть на себе зобов'язання забезпечувати їх неухильне дотримання.

Підписанням цього Акту користувач підтверджує обов'язок виконання пункту 4.4.2 цього Порядку.

Члени робочої групи:

_____ (П.І.Б.) _____ (підпис)
 _____ (П.І.Б.) _____ (підпис)

Акт надіслано ТОВ «Д.І.О. – ТРЕЙДЕР ІНТЕРНАЦІОНАЛ» «__» _____ 20__ року.

*Термін дії цього Акту – 2 роки з дати його затвердження