

ТЕХНІЧНІ ВИМОГИ (TRD)

**до розробки інформаційно-аналітичної системи об'єктів
нерухомого майна для забезпечення внутрішньо переміщених
осіб житлом**

Шифр розробки: TRD-IASOONM-VPO-06052025-01

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ	8
1.1. Вступ	8
1.2. Підстава для розроблення та найменування сторін	8
1.3. Найменування засобу інформатизації	9
1.4. Мета створення засобу інформатизації	9
1.5. Терміни, що використовуються	9
2. ПРИЗНАЧЕННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ	13
2.1. Основні завдання та функції засобу інформатизації	13
2.2. Очікувані результати від впровадження засобу інформатизації	15
3. ХАРАКТЕРИСТИКА ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ	15
4. ДЖЕРЕЛА РОЗРОБКИ	16
5. ВИМОГИ ДО ЗАСОБУ ІНФОРМАТИЗАЦІЇ	18
5.1. Вимоги до структури та функціонування засобу інформатизації	18
5.1.1. Вимоги до архітектури системи	18
5.1.2. Вимоги до середовища розробки	19
5.1.3. Вимоги до бази даних	20
5.1.3.1. Вимоги до проектування БД	20
5.1.3.2. Вимоги до розробки БД	21
5.1.3.3. Вимоги до документування БД	22
5.1.4. Вимоги до системи логування	23
5.1.5. Вимоги до системи моніторингу	23
5.1.6. Вимоги до технологічного стеку	24
5.1.7. Вимоги до організації реєстрів та профілів візуалізації	26
5.1.7.1. Організація реєстрів в системі	26
5.1.7.2. Організація профілів візуалізації в системі	28
5.2. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи	28

5.3. Вимоги до безпеки.....	29
5.4. Вимоги до ергономіки та технічної естетики	32
5.5. Вимоги до стандартизації та уніфікації.....	34
5.6. Вимоги до надійності засобу інформатизації та збереженості інформації.....	34
5.7. Вимоги до потужності	36
5.8. Вимоги до інтерфейсу користувача	37
5.9. Вимоги до захисту від несанкціонованого доступу	38
5.10. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації та іншими системами.....	39
5.11. Вимоги до режимів функціонування засобу інформатизації.	42
5.12. Вимоги до логування дій.....	43
5.13. Вимоги до патентної чистоти	43
5.15. Вимоги до функцій (завдань), що виконуються засобом інформатизації	44
5.15.1. Користувачі системи.....	44
5.15.2. Рольова модель.....	45
5.15.3. Високорівневі бізнес-вимоги	47
5.15.4. Опис цільових бізнес-процесів.....	48
5.15.4.1. Реєстрація користувачів та отримання ролей	49
5.15.4.1.1. br-01. Реєстрація користувачів	49
5.15.4.1.2. br-02. Отримання ролі члена комісії або учасника ТРГ.....	52
5.15.4.1.3. br-03. Додавання категорій користувача	55
5.15.4.1.4. br-04. Додавання уповноважених осіб	58
5.15.4.1.5. br-05. Вхід в систему зареєстрованого користувача з багаторольовим доступом	60
5.15.4.2. Адміністрування системи.....	63
5.15.4.2.1. br-06. Блокування доступу до електронного кабінету.....	63
5.15.4.2.2. br-07. Анулювання доступу до електронних	

кабінетів.....	65
5.15.4.2.3. бр-08. Автоматичне анулювання доступу до електронного кабінету.....	67
5.15.4.2.4. бр-09. Відновлення доступу до електронних кабінетів.....	69
5.15.4.3. Робота з відомостями про координаційну комісію/комісію з обстеження.....	71
5.15.4.3.1. бр-11. Внесення в систему відомостей про уповноважених осіб місцевих державних (військових) адміністрації.....	71
5.15.4.3.2. бр-12. Додавання відомостей про координаційну комісію/комісію з обстеження.....	73
5.15.4.3.3. бр-13. Внесення відомостей про зміни до складу координаційної комісії/комісії з обстеження.....	75
5.15.4.4. Робота з відомостями про Тимчасову робочу групу координаційної комісії/комісії з обстеження.....	79
5.15.4.4.1. бр-15. Додавання відомостей про Тимчасову робочу групу координаційної комісії/комісії з обстеження.....	79
5.15.4.4.2. бр-16. Внесення змін до складу Тимчасової робочої групи координаційної комісії/комісії з обстеження.....	81
5.15.4.5. Робота зі здійснення обліку ОНМ.....	84
5.15.4.5.1. бр-18. Внесення відомостей рішення про необхідність проведення обстеження ОНМ.....	84
5.15.4.5.2. бр-19. Внесення в систему відомостей актів обстеження ОНМ.....	88
5.15.4.5.3. бр-20. Розгляд актів обстеження нерухомого майна, складених комісіями з обстеження.....	90
5.15.4.6. Робота з матеріалами роботи комісій, які були складені до моменту запуску системи.....	94
5.15.4.6.1. бр-21. Внесення матеріалів роботи комісії, які були складені до моменту запуску системи.....	94
5.15.4.7. Робота неавторизованого користувача з порталом	96

5.15.4.7.1. бр-22. Робота неавторизованого користувача з порталом	96
5.15.4.8. Робота з заявами про надання ОНМ для проживання ВПО	99
5.15.4.8.1. бр-23. Подання заяв про надання ОНМ для проживання ВПО	99
5.15.4.8.2. бр-24. Робота з заявами ВПО	100
5.15.4.9. Робота зі статусами ОНМ	103
5.15.4.9.1. бр-25. Робота зі статусами ОНМ	103
5.15.4.10. Робота з програмно-апаратними та/або методологічними помилками	105
5.15.4.10.1. бр-26. Подання повідомлення про виявлену програмно-апаратну та/або методологічну помилку ...	105
5.15.4.10.2. бр-27. Робота з повідомленнями про виявлену програмно-апаратну та/або методологічну помилку ...	108
5.15.5. Опис моделі даних	110
5.15.5.1. Загальна структура	110
5.15.5.2. Основні сутності	110
5.15.5.2.1. Мета модель	111
5.15.5.2.2. Ідентифікація та доступ	111
5.15.5.2.3. Організації та повноваження	111
5.15.5.2.4. ВПО та користувачі	112
5.15.5.2.5. Об'єкти нерухомості	112
5.15.5.2.6. Документи та підпис	113
5.15.5.2.7. Інші сутності	113
5.15.5.3. Ключові зв'язки між сутностями	113
5.15.5.3.1. Ідентифікація та доступ	113
5.15.5.3.2. Організації та повноваження	114
5.15.5.3.3. ВПО та користувачі	114
5.15.5.3.4. Об'єкти нерухомості	114
5.15.5.3.5. Документи та підпис	115
5.15.5.3.6. Інтеграції та контроль	115

5.15.5.4. Технічні вимоги	115
5.15.6. Документи в системі	116
5.15.7. Функціональні компоненти.....	117
5.15.7.1. МОДУЛЬ “АВТОРИЗАЦІЯ КОРИСТУВАЧІВ”	117
5.15.7.1.1. Опис та призначення	117
5.15.7.1.2. Функціональні вимоги	118
5.15.7.2. +МОДУЛЬ “ЕЛЕКТРОННИЙ КАБІНЕТ”	119
5.15.7.2.1. Опис та призначення	119
5.15.7.2.2. Опис функцій основних складових електронного кабінету.....	120
5.15.7.2.3. Електронний кабінет уповноваженої особи МДА	121
5.15.7.2.4. Електронний кабінет координаційної комісії	123
5.15.7.2.5. Електронний кабінет комісії з обстеження....	124
5.15.7.2.6. Електронний кабінет учасника Тимчасової робочої групи Координаційної комісії	125
5.15.7.2.7. Електронний кабінет учасника Тимчасової робочої групи комісії з обстеження	126
5.15.7.2.8. Електронний кабінет Держателя.....	127
5.15.7.2.9. Електронний кабінет Адміністратора	128
5.15.7.2.10. Електронний кабінет Технічного адміністратора	129
5.15.7.2.11. Електронний кабінет Власника ОНМ.....	129
5.15.7.2.12. Електронний кабінет Орендаря.....	130
5.15.7.2.13. Електронний кабінет ВПО	131
5.15.7.3. МОДУЛЬ “ПОРТАЛ”	132
5.15.7.3.1. Загальні відомості	132
5.15.7.3.2. Функціональні вимоги.....	133
5.15.7.4. МОДУЛЬ “ДОКУМЕНТИ ТА ФАЙЛИ”	134
5.15.7.4.1. Загальні відомості.....	134
5.15.7.4.2. Типові користувацькі сценарії	136
5.15.7.5. МОДУЛЬ “ДОВІДНИКИ ТА КЛАСИФІКАТОРИ	141

5.15.7.5.1. Опис та призначення	141
5.15.7.6. МОДУЛЬ “АДМІНІСТРУВАННЯ”	142
5.15.7.6.1. Опис та призначення	142
5.15.7.6.2. Функціональні вимоги	143
5.15.7.7. МОДУЛЬ “ГІС-СЕРВЕР”	144
5.15.7.7.1. Опис та призначення	144
1.1.1.1.1. Функціональні вимоги	144
5.15.7.8. МОДУЛЬ “ЗОВНІШНІ ІНТЕГРАЦІЇ”	146
5.15.7.8.1. Опис та призначення	146
5.15.7.8.2. Інтеграція з ДІЯ	146
5.15.7.8.3. Інтеграція з ІСЕІ	146
5.15.7.8.4. Інтеграція з ЄІССС	148
5.15.7.8.5. Інтеграція з ЄДР	149
5.15.7.8.6. Інтеграція з ЄДРА та ЄДРАТО	150
5.15.7.8.7. Інтеграція з РБС	151
5.15.7.8.8. Інтеграція з ДРРП	152
5.15.7.8.9. Інтеграція з ІКІС ПФУ	153
5.15.7.8.10. Інтеграція з ДЗК	154
5.15.7.8.11. Інтеграція з Єдиним державним веб-порталом відкритих даних	155
5.15.7.9. МОДУЛЬ “СМС”	156
5.15.7.9.1. Опис та призначення	156
5.15.7.10. МОДУЛЬ “ВА”	156
5.15.7.10.1. Опис та призначення	156
5.15.7.11. МОДУЛЬ “ДОКУМЕНТАЦІЯ”	157
5.15.7.11.1. Опис та призначення	157

6. ВИМОГИ ДО СУПРОВОДУ ТА ОБСЛУГОВУВАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ	158
6.1. Вимоги до гарантійної підтримки	158
6.2. Вимоги до навчання користувачів	159
6.3. Вимоги до документації	160
7. ВИМОГИ ДО ПРИЙМАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ	162

7.1. Вимоги до проведення випробувань	162
7.2. Вимоги до передачі результатів виконаних робіт	162

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Вступ

Інформаційно-аналітична система обліку об'єктів нерухомого майна для забезпечення внутрішньо переміщених осіб житлом (далі - Система) призначена для автоматизації процесів та процедур, пов'язаних із збиранням, накопиченням, обробленням та оприлюдненням інформації про об'єкти державної, комунальної та приватної форми власності, які використовуються або можуть бути використані (за умови їх реконструкції та/або переобладнання) для проживання ВПО, а саме: земельні ділянки, житлові будинки, будівлі, споруди (їх окремі частини), квартири, житлові та нежитлові приміщення, інші ОНМ.

Розробка цієї системи здійснюється на виконання вимог Закону України "Про внесення змін до деяких законів України щодо додаткових заходів, пов'язаних із забезпеченням внутрішньо переміщених осіб житлом".

Основним призначенням даного документу є визначення чітких функціональних, технічних та експлуатаційних характеристик Системи, що дозволить уніфікувати підходи до її проектування, розробки, впровадження та експлуатації, забезпечити сумісність з іншими інформаційними системами, відповідність діючим нормативно-правовим актам, а також гарантуватиме надійну, безпечну та ефективну роботу системи для досягнення цілей державної політики у сфері підтримки ВПО.

1.2. Підстава для розроблення та найменування сторін

Роботи з розроблення Технічних вимог (цей документ) виконані на підставі договору від 30.04.2025 РО098853

Замовник: Управління Верховного комісара ООН у справах біженців в Україні.

Бенефіціар: Міністерство розвитку громад та територій України.

Виконавець: ДП «Науково-дослідний інститут геодезії і картографії».

1.3. Найменування засобу інформатизації

Повне найменування: Інформаційно-аналітична система обліку об'єктів нерухомого майна для забезпечення внутрішньо переміщених осіб житлом.

Скорочене найменування: ІАС ООНМ ВПО, Система.

Шифр роботи: TRD-IASOONM-VPO-29072025-01

1.4. Мета створення засобу інформатизації

Метою створення ІАС ООНМ ВПО є підвищення ефективності, прозорості та керованості процесів обліку, аналізу та використання ОНМ. У підсумку Система покликана стати єдиною інформаційно-аналітичною системою для формування та підтримки державної політики у сфері оперативного забезпечення ВПО житлом.

1.5. Терміни, що використовуються

В даній роботі використовуються терміни та скорочення, наведені в таблиці нижче.

Таблиця. Терміни, скорочення та їх визначення

Термін/Скорочення	Визначення
BRD	Business Requirements Document (документ бізнес-вимог)
BPMN	Business Process Model and Notation (Нотація та модель моделювання бізнес-процесів)
Use Case	Опис взаємодії між користувачем (актором) і системою для досягнення певної цілі
Авторизація	Електронна процедура встановлення рівня прав доступу до різних підсистем та модулів ІАС
ДЗК	Державний земельний кадастр
ДРРП	Державний реєстр речових прав на нерухоме

	майно
ІАС ООНМ ВПО, Система	Інформаційно-комунікаційна система, призначена для автоматизації процесів та процедур, пов'язаних із збиранням, накопиченням, обробленням та оприлюдненням інформації про об'єкти державної, комунальної та приватної (за згодою власників) форми власності, які використовуються або можуть бути використані чи реконструйовані, переобладнані для проживання внутрішньо переміщених осіб, а саме: земельні ділянки, житлові будинки, будівлі, споруди (їх окремі частини), квартири, житлові та нежитлові приміщення, інші об'єкти нерухомого майна
ОНМ	Об'єкти державної, комунальної та приватної форми власності, які використовуються або можуть бути використані чи реконструйовані, переобладнані для проживання ВПО, а саме: земельні ділянки, житлові будинки, будівлі, споруди (їх окремі частини), квартири, житлові та нежитлові приміщення, інші об'єкти нерухомого майна
ЕП	Електронний підпис (КЕП або УЕП)
ЕК	Електронний кабінет
ВПО (IDP)	Внутрішньо переміщені особи (Internally Displaced Persons)
ПФУ	Пенсійний фонд України
ПЗ	Програмне забезпечення
ТРГ	Тимчасова робоча група (координаційної комісії або комісії з обстеження)

Електронні документи	Документи, створені або внесені в електронній формі до ІАС, інформація в яких зафіксована у формі електронних даних, включаючи обов'язкові реквізити документа, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису
Екстент (карти)	Прямокутна область на карті, що визначає її початкові межі відображення (географічний діапазон координат, який користувач бачить при завантаженні карти).
ОМС	Орган місцевого самоврядування - виборні та інші органи територіальних громад, наділені повноваженнями вирішувати питання місцевого значення
РН	Реєстраційний номер (документу), що застосовується для ідентифікації в системі
ОДА/ОВА	Обласна державна (військова) адміністрація
РДА/РВА	Районна державна (військова) адміністрація
ЄІБД ВПО	Єдина інформаційна база даних про внутрішньо переміщених осіб
ЄДРА	Єдиний державний реєстр адрес
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
ЄДРАТО	Єдиний державний реєстр адміністративно-територіальних одиниць
ЄІССС	Єдина інформаційна система соціальної сфери
Користувач	Державний орган, місцева держадміністрація

електронного кабінету	(військова адміністрація), орган місцевого самоврядування, інша юридична або фізична особа, яким надається доступ до електронного кабінету та які пройшли процедуру електронної ідентифікації та автентифікації
Користувач системи	Фізична або юридична особа, яка користується інформацією, оприлюдненою на порталі
Методологічна помилка	Невідповідність методології та/або алгоритмів роботи системи положенням законодавства (зокрема невідповідність відомостям (даним) у документах)
Програмно-апаратна помилка	Помилка, недолік або дефект у програмному забезпеченні або програмних складових частинах, програмно-апаратному устаткуванні, каналах зв'язку, функціонуванні засобів електронного підпису, що призводить до неправильного або неочікуваного результату, або неочікуваної роботи чи унеможлиблює роботу системи
Орендарі об'єктів освіти	Державні та комунальні підприємства, громадські об'єднання, благодійні організації, які є орендарями будівель, споруд, приміщень (їх окремих частин) закладів і установ освіти державної та комунальної форми власності з метою надання зазначеного майна для тимчасового проживання внутрішньо переміщених осіб.
Шар (layer)	Посилання на колекцію географічних даних, до яких можна отримати доступ і які можна відобразити на веб-карті чи сцені. Існують

	шари базової карти та шари даних які мають векторний або растровий формат.
CRUD-операції	Create (Створити), Read (Читання), Update (Редагування) та Delete (Видалення). Це чотири фундаментальні операції, які становлять основу керування даними в програмуванні, базах даних та системах зберігання інформації.

2. ПРИЗНАЧЕННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

2.1. Основні завдання та функції засобу інформатизації

Функціональними можливостями Системи має забезпечується виконання наступних завдань:

- електронна ідентифікація та автентифікація користувачів ЕК, зокрема з використанням інтегрованої системи електронної ідентифікації, ЕП, що базується на кваліфікованому сертифікаті відкритого ключа, або іншого засобу електронної ідентифікації із середнім або високим рівнем довіри, які дають змогу однозначно встановлювати особу та здійснення процедури авторизації з метою визначення його ролі в системі і відповідного рівня доступу до інформації";
- здійснення дій з боку користувачів ЕК в частині внесення, завантаження та збереження в системі інформації, документів, фото- та відеоматеріалів, що стосуються або пов'язані з ОНМ (зокрема відомості (дані) щодо техніко-економічних показників ОНМ, актів комісій з обстеження та додатків до них, відомостей, що містяться в них, у тому числі щодо можливості/неможливості використання ОНМ для проживання ВПО, тощо);
- автоматизація процесів та процедур, пов'язаних із збиранням, накопиченням, обробленням та оприлюдненням інформації про ОНМ з метою її верифікації та актуалізації задля ведення обліку ОНМ;

- ведення обліку ОНМ, які використовуються або можуть бути використані для проживання ВПО, систематизації інформації про такі об'єкти;
- подання та розгляду в порядку, встановленому Кабінетом Міністрів України, заяв внутрішньо переміщених осіб про надання їм для проживання об'єктів нерухомого майна, відомості про які містяться в Системі;
- автоматична фіксація (логування) всіх дій будь-яких користувачів системи та користувачів ЕК з часовими відмітками у журналі дій Системи;
- реалізація перевірки повноти та захищеності інформації та електронних документів, які містяться в Системі, від несанкціонованих змін;
- підключення до системи електронної взаємодії державних електронних інформаційних ресурсів "Трембіта";
- управління правами доступу до інформації та електронних документів;
- захист інформації та електронних документів, що обробляються в системі, відповідно до вимог законодавства у сфері захисту інформації;
- CRUD-операції та пошук інформації через електронний кабінет
- публікація, пошук та перегляд інформації та електронних документів в системі, що підлягають оприлюдненню відповідно до Закону України "Про доступ до публічної інформації";
- пошук та перегляд аналітичної та статистичної інформації, що міститься та обліковується в системі;
- відображення на інтерактивній карті порталу ОМН, даних про ОНМ, забезпечення пошуку та перегляду даних ОНМ на допомогою інструментів порталу
- інші функціональні можливості, визначені цим документом.

2.2. Очікувані результати від впровадження засобу інформатизації

Реалізація створення Системи має на меті забезпечити ефективний, прозорий та сталий процес ведення обліку об'єктів нерухомості, які

використовуються або можуть бути використані для тимчасового чи постійного проживання внутрішньо переміщених осіб.

Завдяки інтеграції Системи із державними реєстрами та інформаційними системами, а також можливості обміну даними з міжнародними організаціями, забезпечується підвищення прозорості, швидкості та якості прийняття управлінських рішень на всіх рівнях, від територіальних громад і регіональних адміністрацій до центральних органів виконавчої влади.

3. ХАРАКТЕРИСТИКА ОБ'ЄКТА ІНФОРМАТИЗАЦІЇ

Об'єктом інформатизації є облік ОНМ які використовуються або можуть бути використані чи реконструйовані та/або переобладнані для проживання ВПО, а також документи пов'язані з процесом обліку та визначення статусу ОНМ (в частині можливості/неможливості використання ОНМ, наявності або відсутності вільних місць та/або приміщень для проживання ВПО), та обробки заяв ВПО про надання їм для проживання ОНМ, відомості про які містяться в Системі.

Основними процесами, що підлягають інформатизації, є:

- ведення обліку ОНМ, які використовуються або можуть бути використані (після реконструкції та/або переобладнання) для проживання ВПО, систематизації інформації про такі об'єкти;
- забезпечення відкритого доступу до інформації про ОНМ, які надаються або можуть надаватися для проживання ВПО, у тому числі про місцезнаходження таких об'єктів та їх технічний стан:
 - шляхом оприлюднення на порталі, який забезпечує відкритий доступ до відповідної інформації у режимі реального часу, в тому числі у формі загальнодоступної інтерактивної мапи;
 - шляхом оприлюднення на Єдиному державному веб-порталі відкритих даних;
- подання та розгляду в порядку, встановленому КМУ, заяв ВПО про надання їм для проживання ОНМ, відомості про які містяться в Системі;

- залучення ресурсів (у тому числі міжнародної допомоги) для фінансування ОНМ, призначеного для проживання ВПО.

4. ДЖЕРЕЛА РОЗРОБКИ

Основними джерелами розробки даного документу є:

- Закон України №4080-ІХ від 20.11.2024 “Про внесення змін до деяких законів України щодо додаткових заходів, пов’язаних із забезпеченням внутрішньо переміщених осіб житлом”;
- Постанова КМУ від 16.07.2025 №894 “Деякі питання створення, функціонування Інформаційно-аналітичної системи об’єктів нерухомого майна для забезпечення внутрішньо переміщених осіб житлом та її взаємодії з іншими інформаційно-комунікаційними системами”;
- Постанова КМУ від 29.04.2025 №489 “Про затвердження Порядку обстеження об’єктів нерухомого майна для проживання внутрішньо переміщених осіб та типової форми акта обстеження нерухомого майна”;
- Постанова КМУ від 29.04.2025 №493 “Деякі питання організації роботи з обстеження об’єктів нерухомого майна для проживання внутрішньо переміщених осіб”;
- Постанова КМУ від 29.04.2022 №495 “Деякі заходи з формування фондів житла, призначеного для тимчасового проживання внутрішньо переміщених осіб”;
- Постанова КМУ від 19.03.2022 №333 “Про затвердження Порядку компенсації витрат за тимчасове розміщення (перебування) внутрішньо переміщених осіб”;
- Постанова КМУ від 01.09.2023 №930 “Деякі питання функціонування місць тимчасового проживання внутрішньо переміщених осіб”;
- Постанова КМУ від 31.03.2004 №422 “Про затвердження Порядку формування фондів житла для тимчасового проживання та Порядку надання і користування житловими приміщеннями з фондів житла для тимчасового проживання”;

- Постанова КМУ від 22.09.2016 №646 "Про затвердження Порядку створення, ведення та доступу до відомостей Єдиної інформаційної бази даних про внутрішньо переміщених осіб";
- Постанова КМУ від 21.02.2025 №205 "Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації";
- Постанова КМУ від 08.04.2025 №395 "Про внесення змін до Порядку передачі в оренду державного та комунального майна";
- Постанова КМУ від 25.10.2024 №1225 "Про реалізацію експериментального проекту щодо надання субсидії на оплату вартості або частини вартості найму (оренди) житлового приміщення (частини житлового приміщення) та компенсації частини податку на доходи фізичних осіб або єдиного податку та військового збору";
- Постанова КМУ від 11.03.2022 №261 "Про затвердження Порядку та умов надання компенсації за спожиті комунальні послуги під час розміщення внутрішньо переміщених осіб у будівлях (приміщеннях) об'єктів державної, комунальної та приватної власності у період воєнного стану".

Даний перелік не є вичерпний. Вимоги законодавства України, нормативних документів, що стосується мети, призначення та цілей створення Системи можуть бути доповнені.

5. ВИМОГИ ДО ЗАСОБУ ІНФОРМАТИЗАЦІЇ

5.1. Вимоги до структури та функціонування засобу інформатизації

5.1.1. Вимоги до архітектури системи

Архітектура Системи повинна будуватися з дотриманням загальних стандартів веб-технологій як клієнт-серверна система з трирівневою архітектурою, з урахуванням вимог до засобів для підтримки клієнта, веб-серверу із сервером прикладних застосунків та веб-геосервісами, серверу сховища даних із засобами адміністрування веб-сайту (геопорталу)

відповідно до вимог Постанови КМУ №205 від 21 лютого 2025 р. про “Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації”.

З точки зору масштабованості архітектура системи повинна мати:

- можливість апаратного або програмного масштабування у випадку зростання навантаження чи додавання нової функціональності, що пов'язано як зі зростанням кількості документів та/або користувачів, так і зі збільшенням обсягу збереженого вмісту документів та вимог до функцій Системи;
- можливість функціонального поетапного розширення в межах, але не обмежуючись єдиною апаратно-програмною платформою;
- можливість розширення функціональності за рахунок розгортання додаткових модулів Системи.

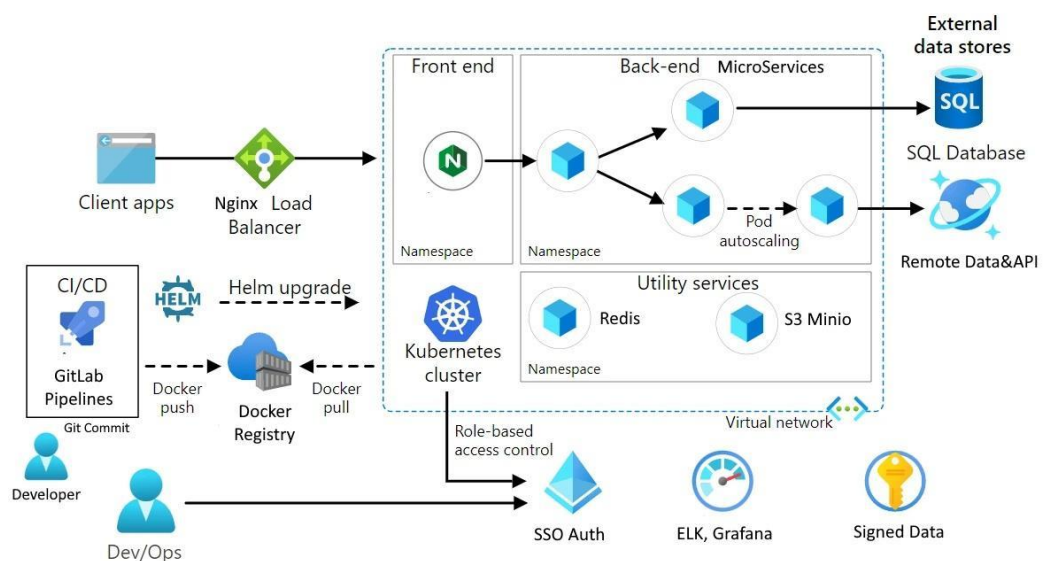


Рисунок. Схема реалізації архітектури

ПЗ має реалізувати наступні взаємодії, а саме:

- обмін інформацією між сервером застосунків і клієнтською частиною та іншими зовнішніми системами повинен бути із застосуванням веб-сервісів;
- компонент серверу застосунків реалізації бізнес-логіки призначено для створення серверних служб доступу до об'єктів та бізнес-логіки прикладної функціональності у відповідності до функціональних задач;

- компонент серверу застосунків сервісів інформаційної взаємодії призначено для забезпечення ведення регламентів взаємодії та механізмів інформаційного обміну;
- компонент серверу застосунків сервісів обробки та управління інформаційними даними призначено для формування, актуалізації даних та виконання запитів до бази даних.

Базові принципи архітектури:

- багаторівнева модульна архітектура: клієнтський рівень > API/BFF(Backend For Frontend) > бізнес-сервіси > дані > інтеграційний шар > спостережність/безпека;
- контрактна взаємодія через відкриті API (REST/JSON, подієві інтеграції);
- stateless web services - кожен запит до сервісу обробляється незалежно, без збереження проміжного стану в пам'яті самого сервера;
- довгі процеси, типу генерація PDF-документу, підписання файлу КЕП, запит до зовнішнього реєстру (ДРПП, ЄДР), пакетна обробка передбачає асинхронні черги;
- просторові дані відокремлені в ГІС-шар (PostGIS, VectorTiles та інші OGC-сервіси);
- єдиний контур ідентифікації (OAuth2/OIDC), ролі/права, журнал подій, шифрування даних/каналів;
- централізовані логи, метрики, трейси; дашборди та алерти;
- горизонтальне масштабування stateless-сервісів, окреме масштабування сховищ, кешування.

Рівень контейнерів.

1. Клієнтські застосунки

- Портал : публічний каталог ОНМ, мапа, перехід на авторизацію в Електронний кабінет, інші реєстри та розділи, що будуть визначені технічним завданням;
- Електронний кабінет: ВПО, Організації/балансоутримувачі, Комісії, Робочі групи, Адміністрування та інші інтерфейси авторизованих користувачів;
- ГІС-клієнт: перегляд/редагування просторових об'єктів (шари, фільтри, вимірювання).

Кожний клієнт працює з Backend-for-Frontend (BFF) шаром для оптимізованих API під конкретний UI.

2. Сервер бізнес-логіки:

- API-шлюз: маршрутизація/захист API, rate-limits, TLS, JWT-перевірки;
- BFF-сервіси: фасади для Порталу, Електронного кабінету, ГІС-клієнта;
- Доменні сервіси:
 - Користувачі/IAM (ролі, права, комісії/ТРГ)
 - Реєстр ОНМ (об'єкти, адреси, власники, ділянки, медіа)
 - Заяви/процеси (оркестрація кроків, валідації)
 - Документи/версії/підписи/сховище
 - Сповіщення/черги/планувальник задач
 - Аналітика/звіти (агрегації, вибірки).
- ГІС-сервіси:
 - Публікація просторових шарів (OGC: WMS/WFS/WMTS/VectorTiles)
 - Рендеринг/кеш тайлів, геокодування.
 - Топологічні операції, просторові фільтри

3. Рівень даних:

- Реляційна БД PostgreSQL реєстрові та транзакційні дані, PostGIS для геопросторових даних;
- Об'єктне сховище файлів (скани, генеровані PDF, підписані архіви);
- Кеш (in-memory) для каталогу/карти/довідників.
- Сховище метрик і логів (time-series для алертингу; централізовані журнали).

4. Інтеграційні сервіси:

- Сервіс інтеграцій/адаптери до зовнішніх реєстрів (ДРПП, ЄДР та ін.), з підтримкою:
 - синхронних викликів (REST/SOAP) і асинхронних черг (вебхуки/черги повідомлень);
 - ETL*/CDC** для періодичних завантажень;

- мепінгу даних і журналу спроб/помилوک.

Примітка 1. Під час розробки технічного завдання, розробнику слід дослідити частоту оновлення даних реєстрів та обмеження на кількість запитів, та встановити ці обмеження під час розробки програмного забезпечення.

Примітка 2. Функція запиту до реєстрів, яка виконується за ініціативи користувача, який має повноваження в межах функціоналу Системи, має бути виконана окремим блоком інтерфейсу електронного кабінету та покриватись рольовою моделлю системи - тобто запит щодо оновлення даних з інтегрованого реєстру має бути окремим системним правом з відповідною роллю, що може бути надана користувачу певного типу адміністратором системи.

- Сервіс підпису: інтеграція з сервісами КЕП/ДЕП (підпис/перевірка, мітки часу).

***Extract, Transform, Load (ETL) – Технологія пакетного обміну або початкового завантаження даних**, яка складається з трьох етапів:

Extract — отримання даних із зовнішніх джерел;

Transform — перетворення структури, очищення та узгодження форматів;

Load — завантаження оброблених даних до внутрішньої бази ІАС.

****Change Data Capture (CDC) – Механізм виявлення та передачі змін у даних між системами в режимі реального часу або з мінімальною затримкою.**

CDC фіксує створення, оновлення та видалення записів у джерельній базі даних і синхронізує лише змінені дані з цільовою системою.

Безпека та доступ:

- Ідентифікація/автентифікація: OAuth2/OIDC, SSO, MFA для адміністраторів.
- Авторизація: RBAC (ролі/права), політики доступу до записів/шарів. + ABAC для реалізації територіальних повноважень, користувачів що працюють на правах

делегованих від обласних та районних адміністрацій. RBAC (роль - дозвіл на дію) + ABAC (атрибути - фільтр доступних даних)

- Шифрування: TLS 1.2+ у каналі; чутливі поля — шифрування at-rest.
- Аудит: незмінні журнали дій (створення/редагування/підпис/експорт).
- Ізоляція мережі: DMZ для публічних компонентів, окремі підмережі для ГІС-ядра і БД.
- Сек'юриті-скан/пентест як частина релізного процесу.
- CI/CD: збірка, тести, перевірки безпеки, розгортання по середовищах (DEV/TEST/STAGE/PROD).

Надійність, масштабування, Disaster Recovery (відновлення системи після аварій):

- Горизонтальне масштабування stateless-сервісів; окреме масштабування ГІС-тайлера і каталогу;
- Реплікація БД, read-replica для репортингу/ГІС-читання;
- Резервне копіювання БД та об'єктного сховища; RPO/RTO згідно з SLA;
- Graceful degradation: при збоях інтеграцій — робота з кеша/черги повторних спроб.

5.1.2. Вимоги до середовища розробки

На період розробки та впровадження Система повинна бути доступна для перегляду та тестування користувачами за допомогою web-сервісів.

З метою покращення експлуатації та тестування Система повинна мати окремі середовища для відображення продуктивного стабілізованого функціоналу та відображення прототипів нового функціоналу, який потребує тестування.

Таблиця. Перелік необхідних середовищ

Середовище	Опис
PROD	Продуктивне середовище.
STAGE	Середовище, яка за конфігурацією та функціональністю

	повторює PROD. Середовище призначено для навчання користувачів.
TEST	Середовище, яка за конфігурацією та функціональністю повторює DEV. Середовище призначено для приймальних тестувань та відтворення інцидентів.
DEV	Середовище для розробки та тестування прототипів функціональності. Використовується для проміжного тестування нової функціональності.

5.1.3. Вимоги до бази даних

5.1.3.1. Вимоги до проектування БД

Проектування БД має відповідати наступним принципам:

1. Розмежування схем даних, де:
 - Схема "System" містить таблиці для довідкової інформації, даних користувачів, логів діяльності та інших допоміжних даних;
 - Схема "Registry" містить офіційні документи та записи, включаючи підписані документи, метадані реєстру, а також будь-які дані, пов'язані з процесами реєстрації.
2. Реалізація механізмів аудиту і журналювання доступу до даних реєстру, де лог дій має містити:
 - IP-адресу з якої прийшов запит;
 - ID користувача в системі;
 - інформація про середовище користувача: операційна система, браузер та його версія, тощо;
 - ідентифікатор бізнес-процесу та/або методу API, що виконує звернення до даних;
 - статус операції з даними.
3. Реалізація можливості масштабованості:
 - проектування схеми таким чином, щоб кожна могла бути незалежно масштабована і оновлена без впливу на іншу;
 - забезпечення можливості додавати нові модулі або функціональність до однієї схеми без ризику порушення цілісності іншої.

5.1.3.2. Вимоги до розробки БД

Розробка БД має відповідати наступним вимогам:

1. Реалізація механізмів синхронізації між схемами для забезпечення узгодженості даних (наприклад, після підписання документів їх копії переносяться до схеми "Registry"). Використання транзакції для забезпечення цілісності даних під час переміщення або копіювання між схемами.
2. Забезпечення механізмів резервного копіювання та відновлення даних для обох схем. Реалізація політики архівування та очищення даних відповідно до вимог законодавства і нормативних актів.
3. Система повинна забезпечувати механізм перевірки валідності електронних цифрових підписів (ЕЦП) під час кожного підписання або створення запису. У схемі Registry зберігається інформація, необхідна для підтвердження автентичності та цілісності даних, а саме відомості про підписанта з сертифіката, відмітка часу та результат перевірки. Формування підпису відбувається виключно на стороні клієнта, закриті ключі не передаються на сервер.

5.1.3.3. Вимоги до документування БД

Документування бази даних має відповідати наступним вимогам:

1. Детальний опис фізичної та логічної структури бази даних, включаючи схеми, таблиці, їхні зв'язки, типи даних та індекси. Опис таблиць бази даних групується по схемам. Разом з описом надається код створення схем, таблиць, індексів, ключів, зовнішніх ключів та інших складових бази даних у форматі SQL.
2. Опис таблиць довідників Системи надається разом із первинною інформацією, що мають містити довідники.
3. Опис поля таблиці бази даних має містити наступну інформацію
 - назва поля;
 - тип;
 - довжина поля (за необхідності);
 - значення за замовчуванням (у разі наявності);
 - опис (опис призначення поля українською мовою);
 - обов'язковість поля;

- унікальність;
 - індексація;
 - маска;
 - обмеження;
 - зовнішні ключі.
4. Опис політик безпеки для кожної схеми, включаючи доступ користувачів, шифрування, аудити та механізми контролю доступу.
 5. Документування процесів синхронізації даних між схемами, включаючи механізми контролю цілісності даних. Опис інструкції щодо резервного копіювання та відновлення даних для кожної схеми.
 6. Документувати API або інших механізмів інтеграції між схемами "System" і "Registry". Опис процесів, що забезпечують узгодженість даних при переміщенні або копіюванні між схемами.
 7. Надання рекомендацій щодо розширення та масштабування бази даних. Документування підходів до роботи з даними користувачів та їх ЕЦП, включаючи сценарії динамічного створення облікових записів і зберігання даних.
 8. Опис процедури моніторингу та управління безпекою для обох схем. Розробка керівництва щодо оновлення, підтримки і масштабування бази даних, включаючи сценарії обслуговування та аварійного відновлення.

5.1.4. Вимоги до системи логування

Система логування повинна забезпечувати можливість технічному адміністратору переглядати події по кожному сервісу та користувачу. Повинно бути забезпечено наскрізне маркування логів для перегляду інформації про події.

Протоколювання подій повинно забезпечуватись за стандартизованим форматом. Конфіденційні дані повинні маскуватись за встановленим форматом.

Збереження часових міток в системі повинно відбуватись в UTC форматі. При відображенні часової інформації кінцевому користувачу система має

конвертувати час у часовий пояс Києва: зимовий час - UTC+02:00 або EET; літній час - UTC+03:00 або EEST.

Перелік подій для логування може бути уточнений в процесі розробки системи. Логи зберігаються в форматі JSON.

5.1.5. Вимоги до системи моніторингу

В межах розробки необхідне підключення до системи моніторингу, яка забезпечує оперативний моніторинг роботи всіх компонентів системи (кількість, поточний стан та ін.), включаючи вільне місце на дисковій системі, навантаження, доступність каналів зв'язку.

5.1.6. Вимоги до технологічного стеку

Система повинна використовувати технології, інструменти та системи бази даних, логування, тощо виключно із відкритим кодом. Для зберігання коду Системи потрібно використовувати сервіс сімейства Git.

Версії мов програмування, фреймворків, бібліотек та сервісів мають мати EOL (end of life) не раніше чим дата підписання договору + 2 роки.

База даних має бути побудована в режимі кластера з передбаченням уникнення можливості збою. Виконавець має зазначити пропозицію щодо технологічного стеку у заявці на участь в конкурсі.

Продукти, на яких повинна базуватися система:

- операційна система типу UNIX з відкритим кодом, версії яких визначені розробниками як Long Term Support(LTS) (Ubuntu 22);
- усі прикладні компоненти системи мають бути запаковані у Docker-контейнери;
- система управління розробкою програмним забезпеченням;
- робота між клієнтським та серверними компонентами має бути реалізована виключно з використанням REST API;
- база даних з відкритим кодом для центрального сховища даних.

За результатами розробки системи та реєстрів Виконавець надає стислий опис використовуваного технологічного стеку із зазначенням версійності та призначення компонентів.

Система повинна забезпечувати час відгуку на запити користувачів не більше ніж 200-500 мілісекунд при середньому навантаженні, яке визначається відповідно до розрахунків наведених у цьому документі.

Під час пікових навантажень час відгуку на інтерактивні запити користувачів не повинен перевищувати 2 секунд. Для стандартних HTTP-запитів (REST API) використовується таймаут до 30 секунд, при цьому система має забезпечувати обробку більшості операцій у межах зазначеного часу відгуку. Для інших протоколів взаємодії (gRPC, event stream, server-sent events) обмеження часу встановлюються відповідно до їх специфікацій і характеру обробки даних.

Система повинна залишатися доступною та функціональною при виникненні збоїв окремих компонентів або обладнання, забезпечуючи мінімальний час простою.

Ключові компоненти системи (сервери, мережеві пристрої, бази даних) повинні мати резервні копії (реплікацію) для забезпечення безперебійної роботи в разі виходу з ладу основного обладнання.

У разі збою основного компонента система повинна автоматично перемикатися на резервний, з мінімальними затримками і без втрати даних.

Система повинна мати механізми автоматичного виявлення збоїв і самовідновлення, а також забезпечувати повідомлення адміністраторів про критичні помилки.

Дані повинні регулярно резервуватися, а в разі аварії система повинна мати можливість швидкого відновлення до попереднього стабільного стану.

Ключові програмні компоненти повинні мати резервні копії або бути розгорнуті на кількох серверах, щоб у разі збою одного з них система могла продовжити роботу.

Дані повинні бути репліковані на кілька незалежних носіїв або в різних географічних локаціях для захисту від втрат у разі збою основного сховища.

Система повинна регулярно перевіряти працездатність резервних компонентів і шляхів перемикання, а також проводити тестування для забезпечення їхньої готовності в разі необхідності.

Система повинна підтримувати можливість горизонтального масштабування, що передбачає додавання нових серверів або інстансів для обробки зростаючого навантаження. Система повинна функціонувати коректно при додаванні або видаленні серверів у кластері.

Система повинна дозволяти вертикальне масштабування, тобто можливість збільшення ресурсів (процесора, пам'яті) на одному сервері без необхідності зміни архітектури системи.

За можливості система повинна підтримувати автоматичне масштабування (auto-scaling) відповідно до зміни навантаження. Це включає автоматичне додавання або зменшення серверів або ресурсів у залежності від поточного рівня навантаження.

У разі очікуваного зростання навантаження на систему (наприклад, у зв'язку з сезонними піками), повинні бути передбачені механізми попереднього планування та налаштування ресурсів для забезпечення необхідного рівня продуктивності.

5.1.7. Вимоги до організації реєстрів та профілів візуалізації

5.1.7.1. Організація реєстрів в системі

Реєстр це структурований каталог даних у складі системи, який забезпечує зручний та керований доступ до інформації про сутності та об'єкти бізнес-процесів. Організація реєстрів призначена для створення єдиного, структурованого та керованого каталогу всіх доступних в системі даних, їх систематизацію, легкий пошук.

В рамках розробки має бути забезпечена реалізація наступних можливостей:

- кожен реєстр може викликатися для перегляду через окремий пункт меню в ЕК користувача, з урахуванням рівнів доступу. Назва пункту меню зазначається в описі функції або сценарія;
- кожен реєстр повинен мати повну та коротку назву. Повна назва зазначається над реєстром на сторінці відображення

таблиці реєстра. Повна назва має дати повне та однозначне розуміння про що реєстр;

- в інтерфейсі ЕК реєстрові дані відображаються у формі таблиці, де у стовпчиках реєстру відображається інформація, яка формується на основі атрибутів сутності у межах кожного запису (рядка);
- при відображенні в інтерфейсі стовпчики таблиці реєстру можуть містити два типи даних
 - простий тип (інформація береться з атрибута сутності);
 - складний тип (значення динамічно формуються за формулою, що об'єднує або обчислює інформацію з кількох атрибутів (власних чи пов'язаних сутностей));
- кожен стовпчик реєстру повинен мати назву. Назва стовпчику може мати назву атрибуту, інформацію з якого відображають в стовпчику;
- для кожного реєстру система має дозволяти користувачу включати чи виключати відображення певного стовпчика в таблиці реєстру;
- для кожного реєстру Система має дозволяти користувачу змінювати порядок виводу стовпчиків в таблиці реєстру;
- для кожного стовпчика Система має дозволяти користувачу змінювати ширину цього стовпчика;
- для кожного реєстру має бути встановлена система фільтрації, де інструмент вибору значень в фільтр певного атрибуту має бути зручним та очікуваним відповідно до типу даних цього атрибуту;
- індивідуальні користувацькі налаштування для кожного реєстру мають зберігатися на серверах системи, щоб забезпечити користувачу звичний інтерфейс незалежно від того, де користувач здійснює вхід в систему;
- всі реєстри повинні мати уніфіковану панель керування діями з об'єктами реєстру. Якщо користувачу відповідно до його прав доступу недоступна певна дія, то відповідну кнопку відображається як недоступний;

- інтерфейс реєстру має надавати можливість здійснювати навігацію по сторінкам реєстру, тобто пейджінг (на одній сторінці відображається таблиця з певною кількістю рядків відповідно до встановленого параметру).

5.1.7.2. Організація профілів візуалізації в системі

В профілі візуалізації має бути відображена повна назва сутності, профіль якої ми відображаємо. Також в профілі може бути задіяно два засоби внутрішньої навігації:

- Вертикальне меню розділів. При виборі певного розділу основна робоча область профілю оновлюється та відображає контент відповідного обраного розділу;
- Горизонтальне меню закладок. При виборі певної закладки основна робоча область оновлюється та відображає контент відповідної закладки, включаючи перелік розділів.

Для сутностей, які в своєму бізнес-процесі передбачають наявність різних редакцій одного основного екземпляру бізнес-об'єкту, горизонтальне меню закладок в такому випадку зарезервовано для відображення саме різних редакцій цього бізнес-об'єкту.

5.2. Вимоги до чисельності та кваліфікації персоналу засобу інформатизації та режиму його роботи

Чисельність персоналу повинна забезпечувати штатний режим експлуатації системи відповідно визначених бізнес-процесів. Режим роботи персоналу встановлюється в посадових інструкціях.

Система повинна надавати можливість збільшення кількості користувачів без доопрацювань та модифікацій та мати можливість управління кількістю одночасних підключень одного користувача до системи (дозволяти або забороняти багатосесійну роботу).

Кваліфікація адміністраторів визначається знанням промислових клієнт-серверних СКБД, серверних систем та інших геоінформаційних комерційних програмних продуктів або продуктів з відкритим кодом, які підтримують специфікації OGC (Open Geospatial Consortium), локальних і глобальних мереж та об'єктно-реляційних баз даних.

5.3. Вимоги до безпеки

Захист інформації в електронній Системі базується на реалізації наступних основних принципів:

- централізоване управління Системою;
- послідовність рубежів захисту інформації;
- адекватність та ефективність захисту;
- збереження захисту під час відмови частин Системи;
- захист засобів безпеки;
- безперервність захисту;
- прихованість захисту.

Інформація в Системі повинна оброблятися із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

Підтвердження відповідності здійснюється в порядку встановленому законодавством.

Роботи щодо забезпечення захисту інформації від несанкціонованого доступу мають проводитися у відповідності до вимог чинного законодавства України з питань технічного та криптографічного захисту інформації.

Вимоги щодо робіт або послуг із захисту інформації виконуються відповідно до законодавства у сферах захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та кіберзахисту.

В той же час, повинні виконуватись передумови щодо її створення, а саме:

- повинно бути розроблено комплект проектної та експлуатаційної документації на Систему, які включатимуть основні принципи захисту, визначені вище, а також вимоги щодо захисту інформації від несанкціонованого доступу;
- Система повинна бути розгорнута у відповідному середовищі функціонування;
- Система повинна бути протестована та готова для експлуатації.

На фізичному рівні мають бути виконані наступні правила:

- фізичний доступ до обладнання повинен бути обмеженим та усі дії повинні бути зафіксовані;
- фізичний доступ до резервних копій Системи повинен бути обмеженим відповідно до процесу адміністрування Системи та усі дії повинні бути зафіксованими;
- Система повинна мати функціонал по обмеженню кількості запитів до ЦБД з метою її захисту від перевантаження;
- Система повинна бути забезпечена ефективними заходами безпеки для захисту від загроз, таких як cross-site scripting (XSS), SQL-ін'єкції та інших потенційних векторів атак;
- Необхідно забезпечити зберігання всіх важливих файлів, конфігурацій, паролів та інших критичних даних виключно в файлах конфігурації, які повинні розташовуватися в ізольованому середовищі. Це середовище має бути належно захищене від несанкціонованого доступу та забезпечувати високий рівень безпеки для запобігання витоку, зміни або втрати цінної інформації;
- Система повинна бути розроблена та сконфігурована відповідно до рекомендацій OWASP TOP-10. Система має мати активний захист від шахрайських дій та забезпечувати фрод-моніторинг, що включає у себе:
- Система повинна мати можливість виявляти аномальну активність користувачів, транзакцій або операцій, що можуть свідчити про шахрайство (фрод). До таких аномалій належать незвичайні шаблони поведінки, часті невдалі спроби авторизації, підозрілі транзакції, в т.ч. описані у окремому процесі, тощо.
- Рівні ризику, де кожна операція повинна оцінюватися за рівнем ризику. Високоризиковані операції повинні підлягати додатковій перевірці, зберігатися з вказанням користувача, дати, типу операції та даних, з якими працював користувач, з можливістю вчинення Адміністратором додаткових дій або автоматичного блокування Системою чи вимогою підтвердження через додаткові канали (наприклад, двофакторна аутентифікація).
- Журнал потенційно шахрайських подій і транзакцій - усі потенційно шахрайські транзакції та дії користувачів повинні

реєструватися в системі для подальшого аналізу та аудиту. Журнал подій повинен містити детальну інформацію про користувача, час, IP-адреси, сесії та інші ключові параметри дій в Системі

- Сповіщення про підозрілу активність, де Система повинна мати функціонал автоматичних сповіщень для Адміністратора та за необхідності інших користувачів у разі виявлення підозрілої активності. Повідомлення можуть бути надіслані засобами Системи, через email, месенджер, SMS або інші канали.
- Періодичний аудит, де Система має дозволяти проводити регулярний аудит фрод-моніторингу для оцінки ефективності існуючих правил та алгоритмів виявлення шахрайства. Система повинна мати можливість оновлення й адаптації механізмів фрод-моніторингу залежно від змін у типах загроз та накопиченої інформації.
- Реакція на інциденти, де в разі підтвердження підозрілої активності або шахрайства система повинна автоматично виконувати дії, такі як тимчасове блокування облікового запису, зниження швидкості виконання операцій користувачем, скасування транзакцій або інші заходи з безпеки. Адміністратор повинен мати інструменти для швидкого реагування на такі інциденти.

5.4. Вимоги до ергономіки та технічної естетики

Загальна побудова веб-інтерфейсу повинна мати зрозумілу логічну модель структури вебсторінок та переходів між ними. Веб-сторінки не повинні бути перевантажені інформаційно-графічними матеріалами. Побудова логічних зв'язків у межах певної функціональності має бути зручна та інтуїтивно зрозуміла.

Усі інтерактивні елементи повинні бути виконані у зручному та зрозумілому подаванні з набором відповідних текстових та/або графічних інформаційних підказок. Веб-сторінки повинні відповідати таким вимогам:

- вміст веб-сторінок структурований, логічний, зрозумілий та легкий для читання;

- форми введення інформації прості та запитують тільки необхідну інформацію;
- поля введення інформації підписані, мають короткі, інформативні та однозначні назви, які розташовуються над полем. Поля введення інформації вирівняні одне під одним, по одному в рядок, ширина поля відповідає вмісту, який вводиться;
- для вибору точної дати (день, місяць, рік) або проміжку дат використовується інтегрований календар або поле з маскою;
- під час введення інформації користувачам надаються помітні та зрозумілі підписи та/або інструкції;
- компоненти веб-сторінок повинні мати зрозумілі назви, навігаційні елементи, які повторюються на багатьох вебсторінках та однаково розташовуються, а компоненти з однаковою функціональністю – мають однакові назви та однаковий дизайн.

Рішення щодо ергономіки повинні забезпечувати:

- зрозумілу логічну побудову інформаційної архітектури з певним набором відповідних графічних, текстових, функціональних компонентів;
- зрозумілу логічну побудову структуру сторінок та розділів, переходів та посилань між ними відповідно до інформаційної архітектури;
- зручну та інтуїтивно зрозумілу побудову логічних зв'язків у межах певної функціональності;
- прості, інтуїтивно зрозумілі інтерфейси робочих місць, які не потребують тривалого навчання роботи з ними;
- форми відображення інформації користувачам, що функціонально орієнтовані на вирішення конкретних завдань;
- мінімальну кількість дій користувача при виконанні завдань в системі, відсутність в екранних формах функціональних можливостей, що не потрібні для виконання завдання, яке поставлене перед користувачем
- вбудовані механізми валідації значень, що визначаються для окремих полів, комбінацій полів (контекстно залежний контроль), контроль значень полів за довідниками /

класифікаторами, а також на відповідність вже введеним даним (базі даних), що реалізовані як на серверній, так і на клієнтській частині;

- вбудовані механізми допомоги внесення та отримання інформації, контекстні підказки;
- інтерактивні елементи у зручному та зрозумілому представленні з набором відповідних текстових та/або графічних інформаційних підказок;
- не перевантаження інформаційно-графічними матеріалами.

Користувач повинен отримати зручний інтерфейс із обґрунтованим набором необхідних інструментів для виконання певних дій, закладених у межах відповідного бізнес-процесу.

Основні вимоги до інформаційно-графічних елементів веб-інтерфейсу:

- коректне типізоване відображення (сумісність) інформації в передостанніх версіях найбільш популярних веб-браузерів;
- схожі операції виконуються з використанням ідентичних графічних елементів у повній відповідності до побудови (структури) інформаційної архітектури рішення;
- графічний і структурний дизайн виконаний з урахуванням плавної зміни розміру вікна веб-браузера. Під час перевищення деякого максимального розміру дизайн передбачає заповнення зайвого місця фоновими матеріалами, які збільшуються без обмежень, наприклад, фонові картинкою однорідної структури.

5.5. Вимоги до стандартизації та уніфікації

Стандартизація та уніфікація функцій Системи має бути забезпечена за рахунок використання сучасних інструментальних програмних засобів, які підтримують єдину технологію проектування та розробки функціонального, інформаційного та програмного забезпечення.

У процесі розробки повинні бути реалізовані вимоги до розробки прикладного програмного забезпечення, які забезпечують процедуру обробки інформації, ідентифікацію програмних модулів та баз даних, типізують в окремі програмні модулі відповідно до свого призначення. Система та її окремі технічні рішення повинні відповідати державним та

міжнародним стандартам щодо реалізації абстрактного типу даних Geometry та SQL доступу до просторових даних.

5.6. Вимоги до надійності засобу інформатизації та збереженості інформації

Надійність елементів Системи повинна бути забезпечена за такими напрямками:

- забезпечення працездатності компонентів Системи;
- збереження даних;
- сумісності технічних засобів та програмного забезпечення.

При цьому повинна вимагатися мінімальна увага до реакції на усунення наслідків відмов компонентів, а також програмно-апаратними засобами повинно бути забезпечене збереження даних.

Програмне забезпечення системи має забезпечувати функціонування в режимі: 24 години на добу, 7 діб на тиждень, 365 (366) днів на рік (за умови безвідмовного функціонування апаратного забезпечення).

Усі функціональні компоненти Системи повинні мати надлишковість за схемою щонайменше N+1 з метою технічного обслуговування та оновлення програмного забезпечення або окремих компонентів без перешкоджання роботі всієї Системи.

Для захисту від помилок у системному ПЗ та прикладному ПЗ має бути створена система резервного копіювання з метою оперативного відновлення робочих конфігурацій ПЗ з резервних копій, оперативної заміни програмно-технічних засобів, що вийшли з ладу.

Максимальний час відновлення працездатності Системи не більше 30 хвилин.

Збереженість інформації на випадок аварій повинна бути забезпечена у повному обсязі. Резервне копіювання повинно забезпечуватися функціональністю, реалізованою в рамках ПЗ Системи та одночасно штатними засобами СУБД, що використовуються.

Для забезпечення резервного копіювання інформації на випадок аварій створюється окремі сховища (сховище). Резервне копіювання має відбуватися з періодичністю, що забезпечує повне збереження та

відновлення даних. Затрати часу на відновлення Системи з урахуванням технічних затримок, підключення до резервного ЦОД та операцією контролю працездатності, повинні бути мінімальними для забезпечення безперервної роботи та не перевищувати однієї доби.

У рамках розробки Системи повинні бути передбачені механізми резервного копіювання Системи, процес резервного копіювання та відновлення Системи після аварій.

Відновлення Системи включає в себе:

- відновлення конфігурацій системного та прикладного програмного забезпечення;
- відновлення інформації про користувачів;
- відновлення даних.

Для забезпечення резервного копіювання:

- налаштовується повний дамп бази даних раз на день;
- раз на годину зберігаються операційні логи.

Для забезпечення відновлення після аварій:

- відновлюється останній повний дамп бази даних;
- спеціальний скрипт забирає до обробки операційні логи (від одного логу з часом, меншим за час повного дампу, до першого логу за часом, пізніше, ніж час аварії) та застосовує їх до часу аварії або встановленого.

Збереження даних має забезпечуватися у випадках:

- вимкнення живлення;
- відмови технічних засобів обробки інформації;
- помилки, збоїв або руйнування програмного забезпечення.

5.7. Вимоги до потужності

Відповідно до поточних даних в Україні створено (або передбачається створення) близько 23 Координаційних комісій та 114 Комісій з обстеження. Потужність системи повинна бути розрахована на обробку відповідної кількості звернень, з урахуванням навантажень, наприклад, пов'язаних з більш активним проведенням обстежень об'єктів у теплу пору року.

Попередні дані для розрахунку навантаження на Систему (пікове навантаження):

- Кабінети внутрішніх користувачів: ~ 100 000 од;
- Навантаження документів за день: ~ 2000 од.

Потужність Системи повинна бути розрахована не тільки з урахуванням безпосередньої взаємодії користувачів в Системі, а також з урахуванням завантаження користувачами файлів та документів в Систему.

У разі неможливості Системи обробити одночасно всі запити від користувачів повинна бути передбачена можливість створення черги запитів і обробка запитів відповідно до створеної черги.

5.8. Вимоги до інтерфейсу користувача

Графічний дизайн повинен бути створений з урахуванням дизайн-системи державних сайтів України (<https://design.gov.ua>), затвердженого постановою Кабінету Міністрів України від 12.06.2019 № 493 “Про внесення змін до деяких постанов Кабінету Міністрів України щодо функціонування офіційних веб-сайтів органів виконавчої влади” або Дизайн системи Дії.

Система повинна відповідати таким основним вимогам:

- основна мова інтерфейсу користувача - українська;
- прості та зрозумілі елементи керування, які не потребують навчання роботи з ними;
- зрозуміла навігація по всіх доступних користувачам ресурсах та поточне положення в структурі Системи;
- можливість з кожної сторінки повернутись на головну сторінку відповідного розділу;
- мінімальна кількість дій для вирішення основних задач цільової аудиторії;
- мінімальна кількість інформації, яку повинен ввести користувач для вирішення задач;
- відсутність функцій, що не потрібні для вирішення основних задач.

Кінцеві користувачі отримують доступ до Системи через веб-сайт, як частини інтерфейсу Системи. Вебсайт має бути адаптивним і коректно масштабуватися на екранах різного розміру.

Для кожної з ролей розробляється інтерфейс кабінету, який пристосований до відповідного набору функцій необхідного для ролі. Інтерфейс має бути адаптований для людей з порушенням зору та відповідати стандартам WCAG та ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021-03), IDT) “Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ”. Перевага надаватиметься рішенням, адаптованим для використання в усіх сучасних браузерях та на різних типах пристроїв, а саме:

- комп'ютер;
- планшет;
- телефон.

5.9. Вимоги до захисту від несанкціонованого доступу

Захист інформації в Системі від несанкціонованого доступу має здійснюватися на всіх етапах її життєвого циклу шляхом впровадження й застосування взаємопов'язаної сукупності організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Для забезпечення захисту інформації від несанкціонованого доступу в Системі необхідне поєднання таких заходів:

- адміністративних та організаційних (охорона систем мережі, особливо систем керування та надання доступів, процес надання доступів, підбір та контроль діяльності персоналу, причетного до адміністрування та налаштування системи);
- програмно-апаратні (використання спеціальних апаратних і програмних засобів, що запобігають або ускладнюють несанкціонований доступ до елементів мережі та до інформації, перевірка відповідності вимогам технічного захисту обладнання, що використовується в Системі, перевірка нестандартної активності користувачів);
- обмеження доступу до різних кабінетів для кожного користувача, відповідно до рольового доступу;

Забезпечити доступ до будь-яких компонентів або функцій Системи, за винятком публічної частини, був можливим лише після проходження процедури авторизації користувача виключно за допомогою Інтегрованої системи електронної ідентифікації (ICEI id.gov.ua).

5.9.1. Вимоги до парольної політики

Парольні політики для адміністраторів мають визначатись у вигляді налаштувань і автоматично контролюватись системою керування контенту. Система має бути захищена від найбільш поширених типів атак. Паролі мають зберігатись і передаватись виключно в шифрованому вигляді.

Інформація, що послаблює інформаційну безпеку (така, як id сесії, id користувача, тощо), не повинна відображатись публічно. Має бути реалізована парольна політика та захист від використання слабких паролів відповідно до NIST Password Policy Guidelines..

5.10. Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами засобу інформатизації та іншими системами

Всі інтеграції з іншими системами мають відбуватися із застосуванням інтерфейсу програмування застосунків з одноманітними архітектурними стилями при проєктуванні API (не змішувати різні архітектурні стилі). Для REST API потрібно дотримуватись архітектурного дизайну REST.

Сервер API повинен:

- забезпечувати публікацію url для перевірки працездатності API (healthcheck);
- перевіряти вхідні дані з обов'язковою перевіркою на відповідність:
 - схемі даних (рівні вкладеності, структура даних);
 - типам даних та форматування (date, url, email, ip і тд.);
 - заповненню обов'язкових атрибутів.

Всі довідникові значення що передаються від Клієнта на сервер повинні перевірятись на допустимі значення ідентифікаторів (чи існує такий ідентифікатор, чи доступний для Клієнта). Для числових значень повинні встановлюватись допустимі мінімальні та максимальні значення,

перевірятись на від'ємні значення і т.д. Текстові значення повинні мати обмеження на максимальну кількість символів.

Результат розробки API передається разом з набором тестових прикладів для проведення перевірки Реципієнтом. Приклади надаються в обмінних форматах для використання з Apache JMeter або Postman. Якщо бізнес-процес вимагає декількох послідовних дій, вони повинні бути описані у «колекціях для тестування».

Оскільки API описується за OpenAPI (Swagger) v3, можливе автоматичне використання цього опису в JMeter, Postman та інших інструментах для генерації тестів.”.

API документується у відповідності до специфікації OpenAPI (Swagger) v3. Необхідно дотримуватись семантики при формуванні відповіді на запит. Коди відповіді HTTP застосовуються згідно стандарту RFC 7231. Кожен код має своє значення, і їх потрібно правильно застосовувати:

- 200-ті - успіх. Всі перевірки пройдено, запит виконано успішно;
- 300-ті - перенаправлення;
- 400-ті - Клієнтські помилки. Невідповідність структури, невідповідність формату, невідповідність специфічним бізнес вимогам, вимогам до унікальності і тд;
- 500-ті - Помилки сервера, помилки в коді програми, яку потрібно виправити. Повертати 500 помилку при штатній роботі програми недопустимо.

Разом з розробленим API виконавець передає результати синтетичних навантажувальних тестів Apache JMeter, а також шаблони тестів для відтворення на майданчику замовника. Тести виконуються не менше 10 хв, або до першого неуспішного запиту. Результати оформлюються як звіти довільної форми які мають обов'язково містити:

- Параметри тестового стенду (CPU, RAM, HDD (SDD));
- Кількість конкурентних користувачів;
- Середню кількість запитів на секунду;
- Показники використання RAM та CPU тестового стенду (htop) до запуску тесту та під час виконання;
- Загальну кількість запитів за час тесту;
- Абсолютну та відносну кількість помилок.

- Авторизація користувачів API.

Токен аутентифікації не повинен бути частиною шляху (path) або рядка запиту (query string). Токен від клієнта передається у окремому HTTP-заголовку Authorization. Ключі API не повинні бути статичними. Період життя ключа задається адміністратором глобально.

Вимоги до документації:

- Визначення всіх ресурсів та методів, які підтримуються API.
- Вказання всіх параметрів, які можуть бути передані в запиті до API.
- Визначення всіх можливих кодів статусу, які можуть бути повернені відповіддю на запит.
- Вказання формату та типу даних, що передаються у запитах та відповідях API.
- Вказання правил аутентифікації та авторизації для доступу до ресурсів API.
- Визначення правил обробки помилок та повідомлень про помилки.
- Версіювання API.
- Визначення параметрів запитів та відповідей, які можуть бути опційними.
- Вказання можливості обмеження частоти запитів до API.
- Вказання можливості використання різних форматів передачі даних (наприклад, JSON або XML).
- Визначення можливості використання різних методів передачі даних (наприклад, GET, POST, PUT або DELETE).
- Вказання можливості підтримки вкладених ресурсів.
- Визначення можливості використання різних типів аутентифікації (наприклад, основаної на токенах або на базі імен користувачів та паролів).
- Визначення можливості використання різних методів обробки даних (наприклад, синхронної або асинхронної).
- Вказання правил валідації даних, які передаються у запитах до API.
- Визначення можливості використання різних методів сортування та фільтрації даних.

- Вказання можливості підтримки пагінації даних.
- Всі параметри запитів та структура відповіді повинна мати опис українською мовою.
- При формуванні опису використовувати приклади максимально наближені до реальності, уникати рандомних наборів символів та використання слів “тестовий опис”, “тестовий приклад” і тд.

5.11. Вимоги до режимів функціонування засобу інформатизації

Експлуатація системи має передбачати такі режими:

- основний режим (режим штатного функціонування системи за своїм призначенням);
- нештатний режим (режим нештатного функціонування системи, наприклад, недоступність даних серверу);
- режим адміністрування (режим здійснення централізованого автоматизованого налагодження та автоматизованого оновлення системи одночасно з роботою решти користувачів у основному режимі або в режимі регламентного обслуговування);
- режим регламентного обслуговування (режим технічного обслуговування та відновлення працездатності технічних засобів системи).

5.12. Вимоги до логування дій

Програмними засобами Системи автоматично вносяться до журналу всі дії та/або події, що здійснюються в системі, зокрема дата і час створення, завантаження, надсилання, отримання інформації та електронних документів з ідентифікацією відправника, отримувача, а також будь-якої зміни та видалення даних, доступних в системі, з використанням кваліфікованої електронної позначки часу.

Журнал всіх дій та/або подій, що здійснюються в системі, зберігається два роки (крім випадків, коли законодавством встановлений інший строк зберігання даних). Після закінчення строку зберігання інформація із журналів всіх дій та/або подій видаляється в автоматичному режимі.

Інформація, що міститься в журналі, може бути отримана через систему у формі електронного документа.

5.13. Вимоги до патентної чистоти

До усіх програмних та технічних засобів, що застосовуються в Системі, повинні бути дотримані умови ліцензійних угод та забезпечена патентна чистота.

Міністерство розвитку громад та територій України є власником прав інтелектуальної власності на програмне забезпечення електронної системи.

Якщо буде з'ясовано, що ПЗ має бути сполучений з іншою системою з використанням протоколу або алгоритму обміну для якого діють обмеження в Україні, дозвіл на застосування такого протоколу або алгоритму повинен отримуватись Виконавцем в компетентних органах перед реалізацією інтерфейсу сполучення та введенням в експлуатацію.

5.14. Вимоги до розвитку та модернізації

Термін можливих доробок та виправлень у разі змін у бізнес-процесах має складати не більше 6 місяців з моменту підписання акту про завершення розробки і розгортання ПЗ на ресурсах набувача.

Гарантована технічна та інформаційна підтримка має становити не менше 6 місяців. Вартість гарантійної підтримки, виправлень та доробок у разі змін у бізнес-процесах має включатись до вартості послуг з розробки сервісів.

Перевага надаватиметься гнучким рішенням, що передбачають можливість адміністратору системи, що пройшов відповідне навчання Виконавця, без залучення розробників вносити зміни до розподілу ролей користувачів, зміни послідовності дій, додавання/видалення деяких дій з процесу, налаштування повідомлень, коригування часових проміжків для задач та інших таймерів, тощо. Подальший розвиток Системи та вимоги до Системи визначається окремими документами.

5.15. Вимоги до функцій (завдань), що виконуються засобом інформатизації

5.15.1. Користувачі системи

Система призначена для роботи різних категорій користувачів, які взаємодіють із нею відповідно до своїх повноважень та ролей в Системі. Доступ до функцій Системи здійснюється через електронний кабінет або портал, залежно від статусу користувача та необхідних операцій. Визначаються наступні категорії користувачів:

- Представники Мінрозвитку;
- Представники ОДА (ОВА);
- Члени координаційних комісій;
- Члени комісій з обстеження;
- Учасники ТРГ координаційних комісії та комісії з обстеження;
- Власники ОНМ або уповноважені ними особи (у тому числі уповноважені представники територіальної громади (утворених нею органів місцевого самоврядування), суб'єктів управління об'єктами державної власності)
- Орендарі будівель, споруд, приміщень (їх окремих частин) закладів і установ освіти державної та комунальної форми власності, що надають для тимчасового проживання ВПО;
- Внутрішньо переміщені особи або уповноважені ними особи;
- Адміністратор системи;
- Технічний адміністратор системи;
- Неавторизовані користувачі системи.

5.15.2. Рольова модель

Рольова модель доступу передбачає підтримку визначення ролей, призначення прав доступу ролям, призначення ролей користувачам, керування ролями та правами, а також керування призначенням ролей користувачам. Модель повинна забезпечувати відповідність повноважень згідно з чинним законодавством та підтримувати контекстну авторизацію за територіальним принципом, що дозволяє обмежувати доступ до даних

і функціоналу залежно від території компетенції користувача (область, район, громада тощо).

Для забезпечення належного рівня захисту даних та гнучкості в управлінні правами доступу в Системі доцільно застосувати гібридну рольову модель, що поєднує елементи ABAC (Attribute-Based Access Control) та RBAC (Role-Based Access Control).

Такий підхід дозволить поєднати чітке закріплення прав за ролями з урахуванням контекстних умов (територія, статус об'єкта, етап бізнес-процесу тощо). Це дасть можливість максимально ефективно реалізувати сценарії, де один і той самий користувач у межах своєї ролі може мати різний рівень доступу залежно від конкретної ситуації, але без втрати прозорості та керованості прав доступу.

Ролі користувачів не повинні бути ексклюзивними. Система має забезпечувати гнучкість у керуванні статусом користувача який є ВПО, враховуючи, що він може змінюватися з часом.

Таблиця. Основні вимоги до рольової моделі

№	Елемент рольової моделі	Опис вимоги
1	Визначення ролей	Система повинна підтримувати чітке визначення користувацьких ролей, що відповідають функціям та рівням доступу, необхідним для роботи з системою.
2	Призначення прав доступу ролям	Кожній ролі має бути призначений визначений набір прав на виконання операцій та доступ до даних (створення, перегляд, редагування, видалення, затвердження, збереження документів тощо).
3	Призначення ролей користувачам	Кожен користувач після успішної автентифікації повинен мати призначену одну або кілька ролей.

4	Керування ролями та правами	Система повинна надавати можливості для створення, редагування та видалення ролей, а також для призначення та відкликання прав доступу. Доступ до цих функцій повинен мати адміністратор системи або відбуватись автоматично засобами системи.
5	Керування призначенням ролей користувачам	Повинна бути реалізована можливість призначення та видалення ролей як вручну адміністратором, так і автоматично на основі подій та статусів у системі.
6	Відповідність повноваженням	Призначені відповідно до ролі права доступу повинні відповідати реальним службовим обов'язкам суб'єктів, визначеними законодавством.
7	Контекстна авторизація	Система повинна забезпечувати авторизацію користувачів на основі територіального принципу та повноважень, обмежуючи доступ до даних і функцій у межах визначеної адміністративно-територіальної одиниці або об'єктів, закріплених за організацією чи користувачем.

Кожна роль повинна мати чітко визначений набір прав доступу до функцій та даних, реалізований відповідно до політик авторизації. Вимоги до рольової моделі можуть уточнюватися та змінюватися у процесі подальшої розробки системи та в разі зміни нормативно-правових актів.

Система також реалізує внутрішній механізм керування ролями та правами користувачів, який функціонує на основі перевірки їхнього статусу через автоматизовані запити до інтегрованих зовнішніх систем і внутрішніх модулів.

Отримані результати перевірки використовуються для підтвердження, актуалізації або зміни ролей користувача. На їх основі формується контекстне середовище ЕК, відповідно системних прав та доступних функціональних можливостей.

Адміністратор має повноваження здійснювати блокування доступу як до всього облікового запису користувача, так і до окремих ЕК, залежно від отриманих підстав. В цілому передбачається два типи блокування доступу:

1. повне блокування облікового запису користувача, що застосовується у випадках компрометації особистих ключів автентифікації, втрати контролю над обліковим записом або інших підстав. х сервісів системи;
2. часткове блокування застосовується у випадках, коли обмеження стосуються лише певного ЕК. У цьому разі користувач зберігає доступ до інших дозволених контекстів.

Система веде облік усіх дій із блокування, зберігає журнал подій і забезпечує анулювання чинних токенів автентифікації лише в межах заблокованого контексту або всієї сесії (залежно від типу блокування та архітектури рішення).

5.15.3. Управління статусами ОНМ

Управління статусами ОНМ забезпечує класифікацію, зміну та відображення поточного стану об'єктів нерухомого майна у реєстрі, а також їх візуалізацію на картографічному шарі Порталу та Електронного кабінету, зокрема налаштування стилів відображення.

Метою функціоналу є:

- підтримка актуальної інформації про придатність (можливість) використання об'єктів для проживання ВПО;
- відображення статусу заселення або наявності вільних місць;
- управління технічним станом або етапом підготовки об'єкта;
- зазначення дати, часу та на підставі якого рішення (дій) надано статус ОНМ.

Система має підтримувати динамічне додавання нових категорій і підвидів статусів без зміни програмного коду. Функціонал реалізується через довідник статусів ОНМ який містить таку орієнтовну структуру: Ідентифікатор статусу, Категорія статусу (верхній рівень), Назва укр./англ., Опис статусу, Ознака активності, Колір/символ для відображення на карті (опційно), Порядок відображення Ролі з правами адміністрування можуть:

- додавати/редагувати категорії та статуси;
- змінювати їхній порядок, колір, описи;
- позначати статуси як “архівні” без видалення з історії;
- створювати групи статусів для автоматизації бізнес-процесів (наприклад, при подачі заяви змінювати статус із “вільний” на “заява на розгляді”).

При розробці технічного завдання, виконавцю розробити таблицю “Автоматичне оновлення статусів”, де будуть міститись дані щодо автоматичних змін статусів у відповідності до етапів бізнес процесу, наприклад:

- після затвердження акта обстеження статус “придатний/непридатний” (можливий/неможливий для використання ОНМ для проживання ВПО) оновлюється автоматично;
- після подання заяви ВПО статус об’єкта змінюється на “заява на розгляді”;
- після погодження заяви ВПО статус об’єкта змінюється на “заселений”;
- після завершення робіт “потребує ремонту” на “потребує обстеження”.
- після проведення обстеження “потребує обстеження” на “придатний / непридатний”
- тощо.

Усі зміни фіксуються в журналі історії статусів із зазначенням дати, користувача, причини та бізнес-процесу на підставі якого змінено статус.

Змінювати статуси можуть лише користувачі, що мають права на CRUD операції в межах своєї організації та територіальної юрисдикції; Користувачі без таких прав бачать статуси лише в режимі “перегляд”.

Всі ОНМ, які присутні у Реєстрі Системи, відображаються на карті Порталу та Електронного кабінету. На карті візуалізуються всі об'єкти, незалежно від статусу, з використанням кольорового маркування / символу (за категорією або конкретним підвидом).

Користувач може фільтрувати відображення за статусом (наприклад, показати лише “вільні” або лише “придатні”). У разі відсутності статусу — застосовується нейтральне позначення “невизначено” (“потребує верифікації (обстеження)”) для щойно створених об'єктів реєстру.

При кліку на об'єкт на карті відкривається скорочена картка ОНМ (pop-up).

Таблиця. Рекомендована форма картки ОНМ на карті

Поле	Опис
Назва об'єкта	текст
КАТОТТГ	код і назва громади та населеного пункту
Адреса	текст
Статуси	поточні статуси з кольоровими позначками
Власник / уповноважена особа	назва організації або ПІБ
Посилання	“Переглянути повну картку ОНМ” → відкриває сторінку у реєстрі ОНМ
Кнопка “Подати заявку	відкриває форму подання заяви ВПО на об'єкт

Візуалізація здійснюється на векторних або растрових шарах підключених як картографічні сервіси.

5.15.4. Високорівневі бізнес-вимоги

Високорівневі бізнес-вимоги є стратегічними твердженнями, які описують цілі, потреби та очікування бізнесу або організації, що мають бути задоволені в результаті реалізації проєкту, і які безпосередньо пов'язані з основними бізнес-цілями:

- Система повинна забезпечити створення та ведення єдиної централізованої бази даних, що агрегує інформацію про ОНМ, з зазначенням його статусу (використовуються або можуть бути використані для проживання ВПО);
- Система повинна забезпечити представникам органів державної влади та місцевого самоврядування, які взаємодіють із системою в межах визначених бізнес-процесів, інтерактивний авторизований доступ до розширених відомостей про ОНМ в межах його статусів та інструменти для пошуку, аналізу і прийняття рішень щодо їх використання для проживання ВПО;
- Система повинна забезпечити подання та розгляд в порядку, встановленому КМУ, заяв ВПО про надання їм для проживання ОНМ, відомості про які містяться в Системі;
- Система повинна надавати картографічний інтерфейс для візуалізації ОНМ та відкритий доступ до інформації про ОНМ, які надаються або можуть надаватися для проживання ВПО, у тому числі про місцезнаходження таких об'єктів та їх технічний стан;
- Система повинна інтегруватися з визначеними державними системами та реєстрами в обсязі, необхідному для реалізації бізнес-процесів.

5.15.5. Опис цільових бізнес-процесів

Цільові бізнес-процеси є визначеною послідовністю логічно пов'язаних кроків або дій, що виконуються у встановленому порядку для досягнення конкретної бізнес-мети або отримання певного цінного результату, який перетворює вхідні дані чи ресурси у вихідні продукти, послуги або інформацію, та часто задіює різних учасників (людей, системи, підрозділи).

Схеми бізнес-процесів наведені в системі умовних позначень (нотації) для моделювання бізнес-процесів BPMN (стандарт моделювання процесів, який має в основі послідовність подій та дій, які мають початок та кінець).

5.15.5.1. Реєстрація користувачів та отримання ролей

Ролі користувачів в Системі не повинні бути ексклюзивними. Система має забезпечувати гнучкість у керуванні статусом користувача, враховуючи, що він може змінюватися з часом. Передбачається дві моделі отримання доступу до відповідних інтерфейсів електронного кабінету:

- самоініційована, де користувач автентифікується в системі та отримує доступ до електронного кабінету з базовим інтерфейсом, в якому він може самостійно ініціювати отримання певної ролі/категорії користувача (напр., «ВПО», «Власник ОНМ» або «Орендар»). Система перевіряє дані через запити до реєстрів та інформаційно-комунікаційних систем (ЄІБД, ДРРП, ЄДР, тощо) у порядку визначеному у [модулі “Зовнішні Інтеграції”](#) та, у разі підтвердження, автоматично надає користувачеві відповідне контекстне середовище;
- попередньо ініційована, де користувач після автентифікації отримує в електронному кабінеті з базовим інтерфейсом запит на підтвердження своєї участі напр. в комісії або ТРГ. Якщо користувач підтверджує свою участь, система автоматично надає йому доступ до відповідного контекстного середовища та призначає пов’язані ролі.

5.15.5.1.1. br-01. Реєстрація користувачів

Основні відомості. Даний бізнес-процес описує послідовність дій, що виконуються з метою створення облікових записів для користувачів, їх ідентифікацію (автентифікацію) та подальшого призначення відповідних ролей та прав доступу (авторизація) згідно з рольовою моделлю системи.

Схема процесу

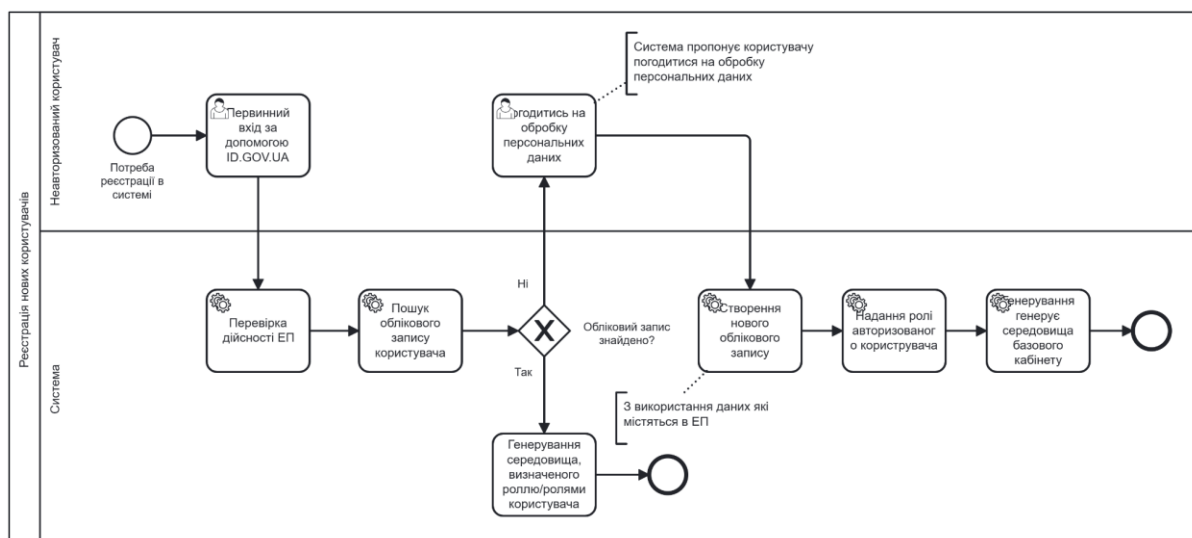


Схема бізнес-процесу. Реєстрація нових користувачів

camunda

<https://modeler.camunda.io/share/b63e4ood-4240-4280-8f3f-94c8da4d571e>

Передумови:

- Користувач не має зареєстрованого облікового запису в системі;
- Користувач має діючий електронний підпис (КЕП або УЕП).

Опис процесу:

- Неавторизований користувач, який раніше не мав облікового запису, здійснює первинний вхід до Системи за допомогою сервісу ID.GOV.UA.
- Система перевіряє дійсність ЕП та здійснює пошук облікового запису користувача за унікальним ідентифікатором (напр. РНОКПП або номер паспорта, що міститься в ЕП).
- Якщо обліковий запис не знайдено, Система пропонує користувачу погодитися на обробку персональних даних та ініціює створення нового облікового запису на основі даних, отриманих з ЕП.
- Система створює базовий обліковий запис користувача, використовуючи дані, що містяться в ЕП та автоматично надає доступ до базового ЕК.
- Система генерує робоче середовище базового Електронного кабінету для користувача, де користувач, в залежності від отриманої ролі, має можливість:

- переглянути відомості профілю користувача та вказати актуальну електронну адресу та дійсний мобільний телефон;
- переглядати профіль організації, до якої відноситься користувач, змінювати організацію від якої працює користувач, якщо користувач відноситься до кількох організацій одночасно. Підтвердити що користувач є керівником організації. У разі підтвердження, що користувач є керівником організації редагувати дані організації, надавати права користувачам на роботу від організації в системі;
- переглянути повідомлення про комісії та/або ТРГ, в склад яких він був попередньо доданий, та підтвердити чи відхилити свою участь в них. В разі підтвердження система формує в кабінеті відповідне контекстне (службове) середовище з наданням відповідної ролі в системі;
- ініціювати отримання категорії користувача (напр. ВПО чи власник ОНМ). Система в такому випадку проводить автоматичну перевірку та надає або відхиляє отримання відповідної ролі з формуванням в кабінеті відповідного контекстного (персонального) середовища (наведено у відповідному бізнес-процесі).

Бізнес-правила:

1. Вхід до Системи здійснюється через ID.GOV.UA.
2. Система перевіряє дійсність ЕП та відхиляє запит у разі виявлення невідповідностей.
3. Створення облікового запису можливе тільки після підтвердження користувачем згоди на обробку персональних даних відповідно до політики конфіденційності та правил обробки персональних даних.
4. Після створення облікового запису система автоматично призначає базову роль користувача та надає доступ до Електронного кабінету з базовим інтерфейсом.

Результат бізнес-процесу. Обліковий запис користувача створено в системі. Користувач успішно увійшов до Електронного кабінету з базовим інтерфейсом, де він має можливість переглянути відомості профілю,

ініціювати отримання категорії користувачів та/або підтвердити участь в роботі комісії та/або ТРГ.

5.15.5.1.2. бр-02. Отримання ролі члена комісії або учасника ТРГ

Основні відомості. Даний бізнес-процес описує послідовність дій, що виконуються з метою підтвердження або відхилення користувачем своєї участі у складі комісій та/або ТРГ, до яких він був попередньо доданий. Процес забезпечує захист від помилкового додавання користувача в комісію та/або ТРГ та автоматичне призначення відповідних ролей. Також процес передбачає можливість відкладеної авторизації члена комісії, яка відбулась **після** додавання в систему відомостей про склад відповідної комісії/ТРГ (наведено в [бр-12](#)).

Схема процесу

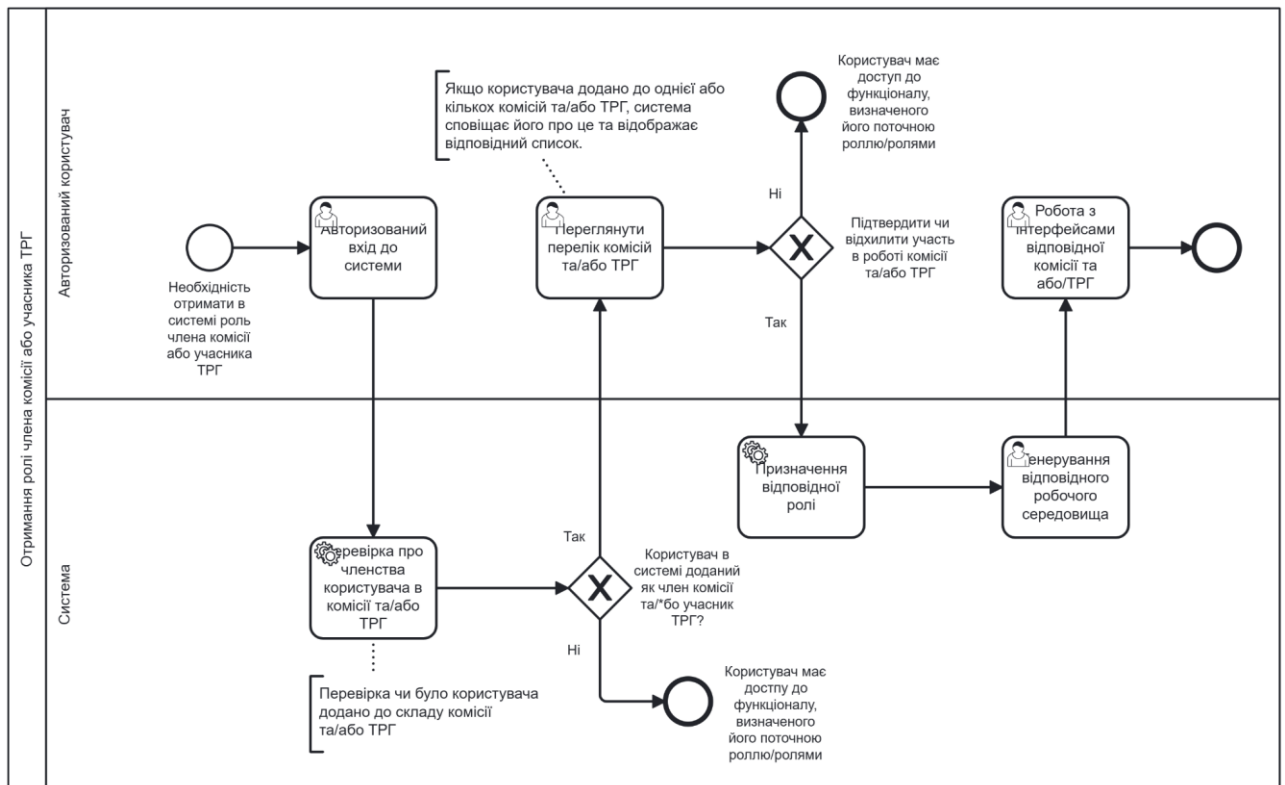


Схема бізнес-процесу. Отримання ролі члена комісії або учасника ТРГ

camunda

<https://modeler.camunda.io/share/6de594af-546a-4dd3-b788-b8dee831b8d7>

Передумови:

- Користувач зареєстрований в системі та має доступ до базового Електронного кабінету.
- Користувач був попередньо доданий до складу однієї або кількох комісій та/або ТРГ (наведено в [bp-12](#)).
- В системі налаштована відповідна рольова модель.

Опис процесу:

- Користувач може бути новим або вже зареєстрованим у системі. Якщо це новий користувач, він проходить процедуру реєстрації та отримує доступ до базового Електронного кабінету. Якщо користувач вже має обліковий запис, він здійснює вхід у систему, після чого система ідентифікує його та завантажує дані профілю.
- Після успішної авторизації система автоматично перевіряє, чи було користувача додано до складу комісії та/або ТРГ. Якщо нових призначень немає, користувач продовжує роботу в середовищі,

визначеному його поточною роллю. Якщо користувача додано до однієї або кількох комісій та/або ТРГ, система сповіщає його про це та відображає відповідний список.

- c. У персональному кабінеті користувач бачить перелік комісій та/або ТРГ, до складу яких він був попередньо доданий та відомості про які було внесено до Системи.
- d. Користувач може підтвердити або відхилити участь у кожній із комісій або ТРГ:
 - в разі підтвердження система автоматично призначає йому роль, що відповідає його функціям у межах конкретної комісії чи ТРГ, та формує службове контекстне середовище, у якому забезпечується доступ до необхідних документів, даних та інструментів;
 - якщо користувач відмовляється від участі, доступ до матеріалів цієї комісії або ТРГ не надається, і він продовжує роботу в середовищі, визначеному його поточною роллю.

Бізнес-правила:

1. Участь у комісіях та/або ТРГ можлива лише після успішної автентифікації користувача в системі.
2. Система призначає ролі автоматично, відповідно до рольової моделі.
3. У разі відмови від участі в комісії та/або ТРГ доступ до її документів не надається.
4. Якщо користувач підтвердив участь хоча б в одній комісії та/або ТРГ, формується відповідне контекстне середовище для роботи з матеріалами кожної підтвердженої комісії та/або ТРГ.
5. У разі появи нових призначень система знову сповіщає користувача та пропонує підтвердити або відхилити участь, після чого виконує автоматичне налаштування ролей і доступів.

Результат бізнес-процесу: Результатом даного бізнес-процесу є успішне підтвердження або відхилення користувачем своєї участі у складі комісії або ТРГ, де в разі підтвердження користувачу призначено роль, створено персональне робоче середовище, надано доступ до даних та

документів, а в разі відхилення - контекстне середовище не створюється, доступ до документів не надається.

5.15.5.1.3. br-03. Додавання ролей користувача

Основні відомості. Даний бізнес-процес описує послідовність дій, що виконуються з метою додавання нових категорій користувача. У межах цього процесу здійснюється перевірка його правового статусу, узгодження з внутрішніми та зовнішніми реєстрами (напр. ЄІБД, ДРРП, ЄДР), а також формування або коригування контекстного середовища ЕК. В рамках процесу додавати можливо лише ролі ініціативної моделі (напр. ВПО, Орендар або Власник ОНМ).

Схема процесу

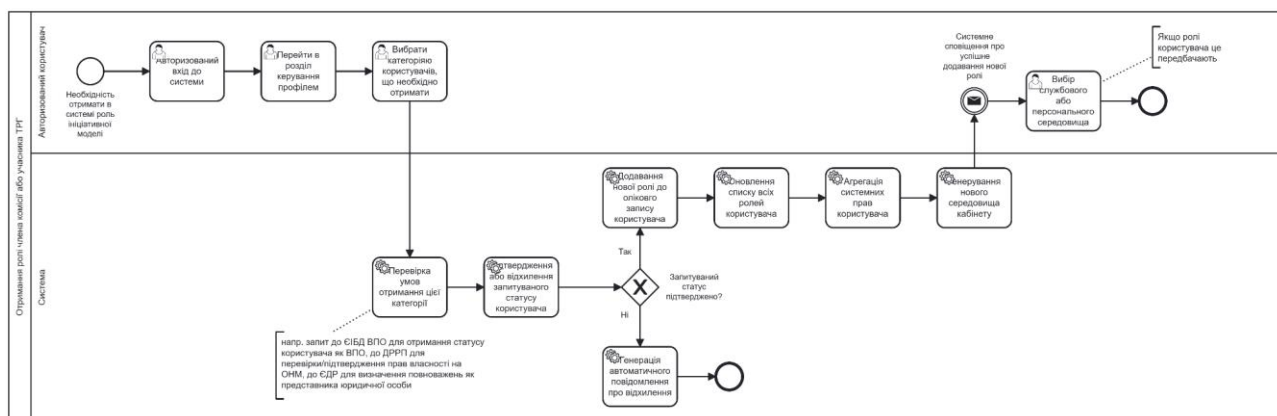


Схема бізнес-процесу. Додавання ролей користувачів

camunda

<https://modeler.camunda.io/share/050ac7ef-e66f-4913-aa49-61fc0cd195f3>

Передумови:

- Користувач зареєстрований у Системі та має обліковий запис.
- Користувач має доступ до ЕК та інтерфейсу керування профілем.
- В Системі реалізована інтеграція з зовнішніми реєстрами та інформаційно-комунікаційними системами (напр. ЄІБД ВПО, ДРРП, ЄДР).
- Налаштована рольова модель, яка дозволяє автоматично призначати та агрегувати права доступу.

Опис процесу:

- Зареєстрований користувач проходить автентифікацію в системі. Система ідентифікує користувача та завантажує дані його поточного

профілю.

- e. Система автоматично спрямовує користувача до Електронного кабінету, де він бачить відповідний персоналізований інтерфейс.
- f. Користувач обирає у відповідній формі (напр. в розділі керування профілем) категорію користувачів яку він хоче отримати, наприклад:
 - ВПО;
 - власник ОНМ;
 - орендар закладу чи установи освіти;
- g. Система виконує автоматичну перевірку умов отримання цієї категорії (напр. запит до ЄІБД ВПО для отримання статусу користувача як ВПО, до ДРРП для перевірки/підтвердження прав власності на ОНМ, до ЄДР для визначення повноважень як представника юридичної особи).
- h. На основі отриманих відповідей, система приймає автоматичне рішення. Якщо статус підтверджено, система переходить до наступного кроку. Якщо статус не підтверджено, система генерує відповідне повідомлення причини відмови та завершує процес.
- i. Система додає нову роль до облікового запису та оновлює список усіх ролей користувача з відповідними правами доступу.
- j. На основі оновленого списку ролей, система агрегує (об'єднує) відповідні системні права та формує нове контекстне середовище електронного кабінету.
- k. Користувач отримує сповіщення про успішне додавання нової ролі та отримує доступ до відповідних функцій ЕК та інтерфейсів системи.
- l. Користувач має можливість вибору службового або персонального контекстного середовища, якщо його ролі це передбачають.

Бізнес-правила:

1. Всі перевірки здійснюються через внутрішні механізми системи та інтеграцію із зовнішніми реєстрами та інформаційно-комунікаційними системами.
2. В разі відсутності підтвердження даних у зовнішніх реєстрах система

відхиляє запит.

3. При додаванні нової ролі система автоматично об'єднує права доступу з усіх активних ролей користувача.

Результат бізнес-процесу: Результатом даного бізнес-процесу є оновлений обліковий запис користувача з успішно підтвердженою та доданою новою роллю, автоматичне розширення його прав доступу та функціоналу електронного кабінету відповідно до цієї ролі, а також формування повідомлення для користувача про успішне завершення операції з можливістю використання нових інтерфейсів і сервісів.

5.15.5.1.4. br-04. Додавання уповноважених осіб

Основні відомості. Цей процес описує послідовність дій, що виконуються з метою додавання в систему відомостей про уповноважену особу, де користувач після автентифікації та авторизації в системі має можливість делегувати права іншій особі, надавши їй відповідну категорію та роль. Після чого уповноважена особа отримує доступ до електронного кабінету з функціоналом, аналогічним відповідній категорії користувача.

Схема процесу

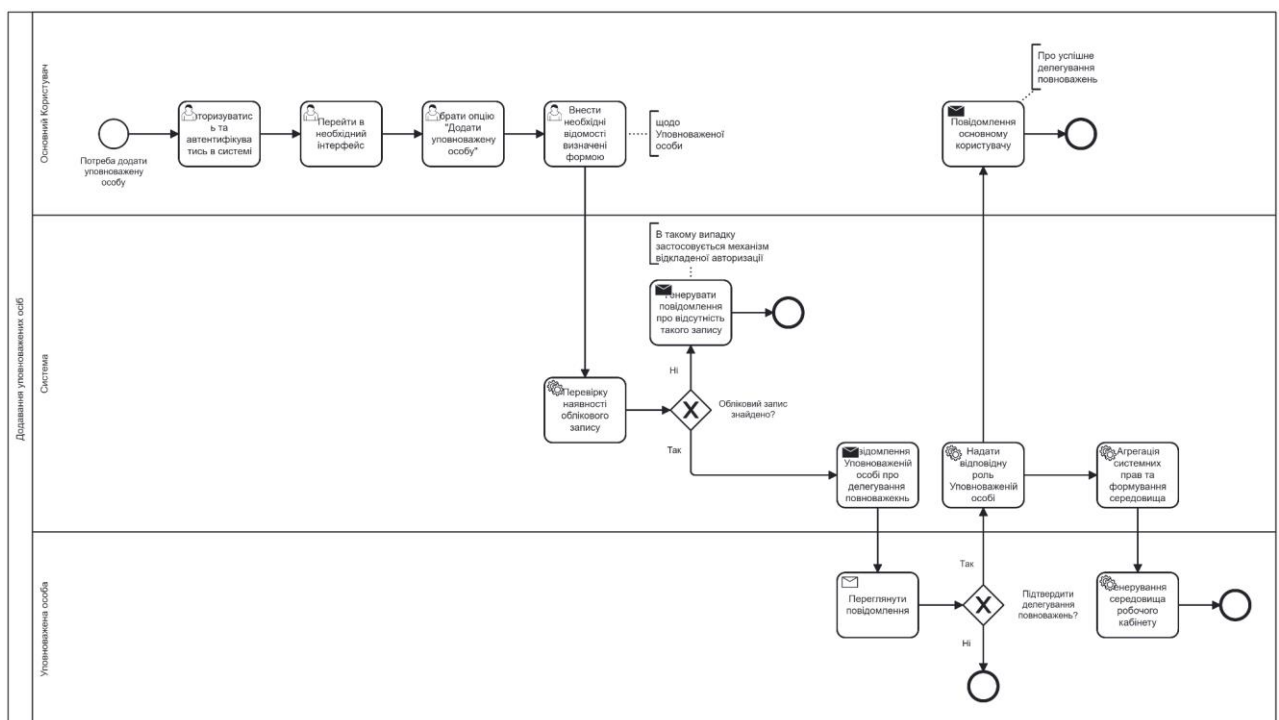


Схема бізнес-процесу. Додавання уповноважених осіб

Передумови:

- Основний Користувач зареєстрований у Системі та має підтверджений обліковий запис.
- Основний Користувач має доступ до електронного кабінету та інтерфейсу керування профілем.

Опис процесу:

- Зареєстрований користувач проходить автентифікацію в Системі. Система ідентифікує користувача та завантажує дані його поточного профілю.
- Система автоматично спрямовує користувача до Електронного кабінету, де він бачить відповідний персоналізований інтерфейс.
- В Електронному кабінеті користувач обирає функцію «Додати уповноважену особу», вказує ідентифікатори уповноваженої особи (напр. РНОКПП) та обирає, від якої категорії користувача або ролі він делегує права.
- Система здійснює перевірку наявності облікового запису. В разі його відсутності застосовується механізм відкладеної авторизації.
- В разі його існування в Системі відповідного облікового запису, уповноважена особа отримує сповіщення у Системі для підтвердження чи відхилення цього статусу.
- В разі відхилення загальний процес завершується. У разі підтвердження Система надає відповідну роль уповноваженій особі, агрегує (об'єднує) відповідні системні права та формує нове контекстне середовище Електронного кабінету для уповноваженої особи.
- Основний Користувач отримує сповіщення про успішне делегування повноважень уповноваженій особі.
- Уповноважена особа має можливість вибору службового або персонального контекстного середовища, якщо його ролі це передбачають. Один користувач може бути уповноваженою особою

одного або декількох користувачів, і переключатись між їх інтерфейсами засобами електронного кабінету.

Бізнес-правила:

1. При додаванні нової ролі система автоматично об'єднує права доступу з усіх активних ролей користувача.
2. Якщо уповноважена особа на момент внесення відомостей про неї не зареєстрована в системі, то застосовується механізм відкладеної авторизації.
3. Основний користувач може відкликати делеговані повноваження.

Примітка. Основний користувач має можливість у будь-який момент відкликати делеговані повноваження уповноваженої особи. Ця дія реалізується через функціонал керування уповноваженими особами в межах ЕК. Після ініціювання відкликання система:

- блокує відповідні доступи та ролі, що були надані уповноваженій особі;
- видаляє або деактивує асоційоване контекстне середовище електронного кабінету уповноваженої особи (без видалення її власного профілю в системі);
- надсилає обом сторонам (основному користувачу та уповноваженій особі) повідомлення про скасування делегування, із зазначенням дати та часу відкликання повноважень.

Уповноважена особа після цього втрачає можливість діяти від імені основного користувача або отримувати будь-які пов'язані з ним повідомлення.

Результат бізнес-процесу: Результатом даного процесу є успішне внесення до системи відомостей про уповноважену особу, якій надано категорію та роль, делеговану основним користувачем, що забезпечує формування для неї персоналізованого електронного кабінету з функціоналом, аналогічним відповідній категорії користувача, та супроводжується автоматичним надсиланням повідомлень обом сторонам про результат операції й доступ до нових сервісів.

5.15.5.1.5. br-05. Вхід в систему зареєстрованого користувача з багаторольовим доступом

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою персоналізованого входу зареєстрованого користувача до системи та надання йому доступу до функціоналу електронного кабінету, що відповідає всім його дійсним ролям.

Схема процесу

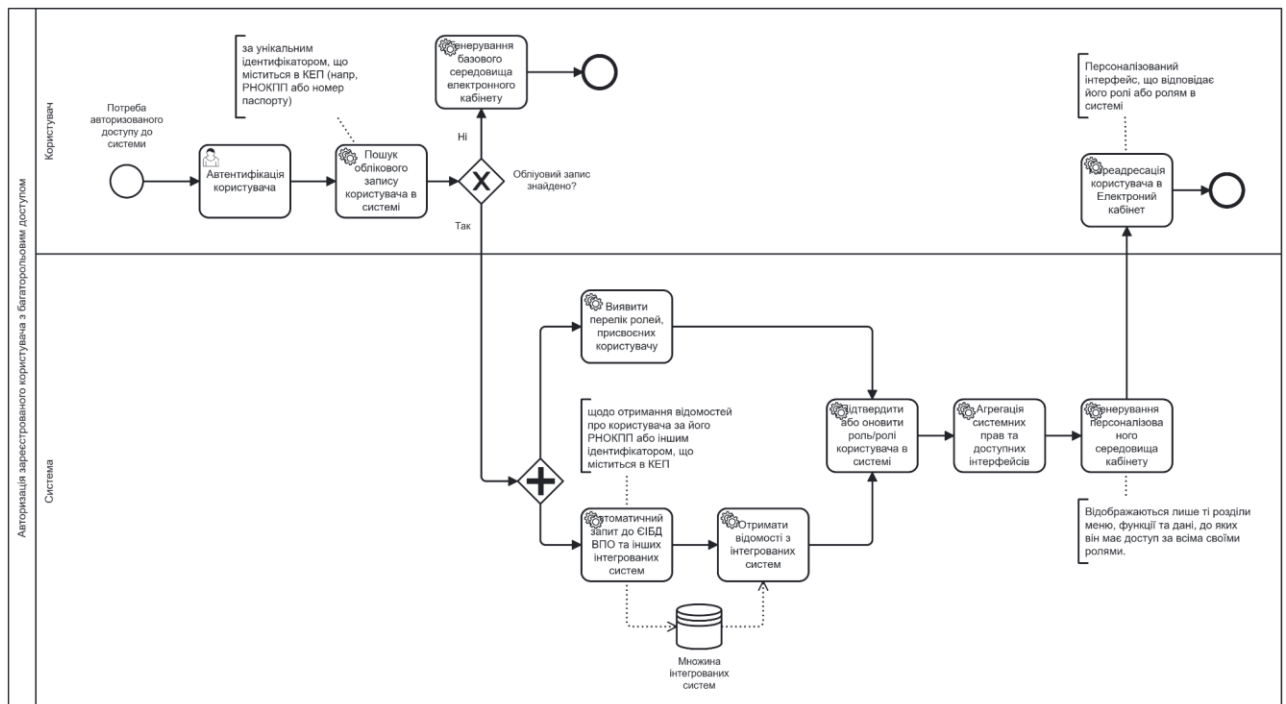


Схема бізнес-процесу. Вхід в систему зареєстрованого користувача з багаторольовим доступом

camunda

<https://modeler.camunda.io/share/94ac14d2-e5f5-4b41-8098-c25a31845fbf>

Передумови:

- Користувач зареєстрований у Системі та має підтверджений обліковий запис.
- Рольова модель користувачів визначена й збережена в Системі, включаючи набір прав доступу для кожної ролі.

Опис процесу:

- Зареєстрований користувач проходить автентифікацію в системі. Система ідентифікує користувача та завантажує дані його поточного профілю.
- Система здійснює перевірку статусу користувача шляхом автоматичного надсилання запитів до інтегрованих зовнішніх систем та внутрішніх модулів. На основі отриманих відповідей Система підтверджує або оновлює ролі та звертається до внутрішнього механізму керування ролями й правами для формування контекстного середовища ЕК, яке містить повний перелік системних прав, що належать відповідному ідентифікованому користувачу. В разі не підтвердження відомостей система генерує відповідне

повідомлення та встановлює відповідний статус.

- c. На основі всіх виявлених ролей, Система агрегує (об'єднує) відповідні системні права доступу (дозволи на перегляд, створення, редагування, видалення, збереження документів) та визначає доступні інтерфейси Електронного кабінету.
- d. Система спрямовує користувача до особистого Електронного кабінету, де він бачить персоналізований інтерфейс, що відповідає його ролі або ролям в системі.
- e. Користувач має можливість перемикання між службовим та персональним контекстними середовищами (напр. у випадку, коли користувач має кілька ролей, що стосуються службових функцій та поданих персональних заяв від фізичної особи).

Бізнес-правила:

- 1. Під час кожної авторизації Система перевіряє дійсність усіх ролей користувача.
- 2. Якщо роль втрачає чинність, Система автоматично відключає пов'язані з нею функції та фіксує її в базі даних для відтворення історії змін доступів.
- 3. Персоналізований інтерфейс формується на основі підтверджених ролей та їхніх прав доступу.
- 4. Користувач може одночасно мати кілька активних ролей, але доступ до даних та функцій Системи регулюється контекстом (службовим або персональним).

Результат бізнес-процесу: Зареєстрований користувач успішно авторизований у системі. Йому надано доступ до персоналізованого Електронного кабінету, що відображає всі доступні інтерфейси та функції відповідно до його підтверджених ролей і прав доступу.

5.15.5.2. Адміністрування доступу до електронного кабінету

5.15.5.2.1. br-06. Блокування доступу до електронного кабінету

Основні відомості. Даний бізнес-процес визначає послідовність дій адміністратора та системи, спрямованих на блокування доступу користувача до Електронного кабінету (без деактивації самого облікового запису). Блокування здійснюється на підставі повідомлень, документів, судових рішень або фактів, що підтверджують необхідність обмеження доступу.

Схема процесу

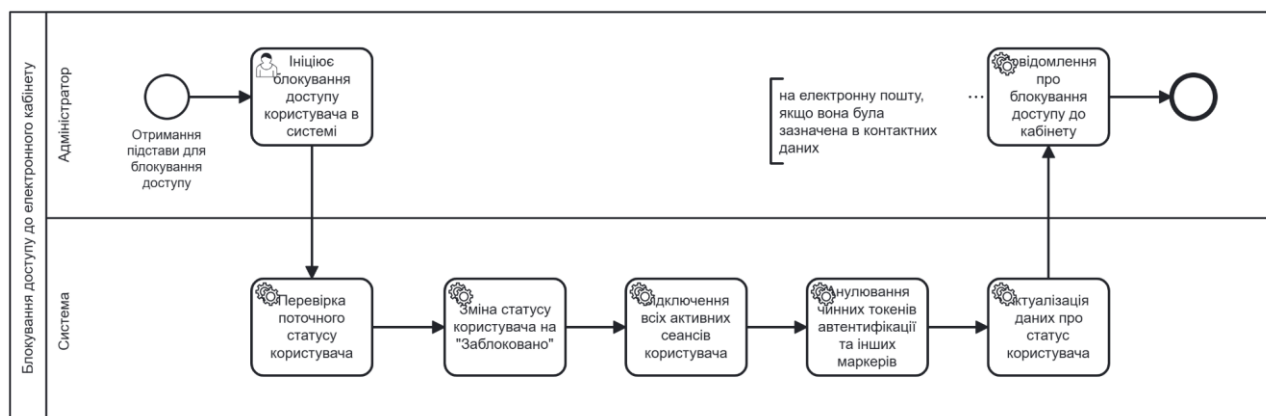


Схема бізнес-процесу. Блокування доступу до електронних кабінетів

camunda

<https://modeler.camunda.io/share/5eb49e66-ac71-4cao-9381-d8bb633b34da>

Передумови:

- Користувач зареєстрований у Системі та має підтверджений обліковий запис.
- У системі визначена роль Адміністратора, який має право виконувати операції з блокування доступу.

Опис процесу:

- Адміністратор отримує підставу для блокування доступу користувача до відповідного ЕК:
 - повідомлення про компрометацію особистого ключа користувача електронних довірчих послуг (від самого

користувача або Держспецзв'язку);

- повідомлення керівника державного органу, місцевої держадміністрації (військової адміністрації) або органу місцевого самоврядування про необхідність блокування доступу у зв'язку з відстороненням посадової особи від виконання посадових обов'язків або відстороненням від посади;
- отримання інформації про внесення користувачем електронного кабінету недостовірної інформації;
- судове рішення про блокування доступу користувача.

b. Адміністратор ініціює процес блокування доступу користувача до відповідного ЕК в системі.

c. Система виконує автоматичні дії з виконання блокування:

- перевіряє поточний статус користувача;
- змінює статус доступу до відповідного ЕК на "Заблоковано";
- завершує активні сеанси у межах заблокованого контексту (інші ролі залишаються активними);
- анулює чинні токени автентифікації та інші маркери доступу, що забезпечують роботу користувача в межах заблокованого контексту або всієї сесії (залежно від архітектури системи).
- актуалізує дані про статус користувача у всіх внутрішніх модулях.
- повертає до інтерфейсу базового облікового запису за умови звернення до заблокованого кабінету.

d. Система формує повідомлення для користувача на його електронну адресу (якщо вона була зазначена в контактних даних) про блокування доступу до Електронного кабінету, із зазначенням причини та, за необхідності, строку дії блокування.

Бізнес-правила:

1. Блокування доступу може виконувати лише користувач із підтвердженою роллю адміністратора.
2. Блокування доступу здійснюється виключно за наявності документально підтвердженої підстави.

3. Користувач зберігає доступ до дозволеного контенту або до функціоналу базового ЕК.

Результат бізнес-процесу: Доступ користувача до Електронного кабінету заблоковано. Система зафіксувала підставу блокування, ініціатора процедури, дату та час застосування обмеження та оновлений статус користувача.

5.15.5.2.2. br-07. Анулювання доступу до електронних кабінетів

Основні відомості. Даний бізнес-процес визначає послідовність дій адміністратора та системи щодо анулювання доступу користувача до ЕК. Анулювання здійснюється на підставі повідомлення керівника уповноваженого органу або судового рішення, що набрало законної сили.

У разі анулювання доступу користувача до ЕК Система не видаляє облікові дані з бази, а змінює статус облікового запису. При цьому всі пов'язані записи (ролі, журнали дій, подані документи, історія доступів) зберігаються у базі даних у стані для читання для забезпечення аудиту та цілісності зв'язків між таблицями.. Надання доступу такому користувачу здійснюється лише шляхом повторної реєстрації користувача та проходження повної процедури автентифікації і присвоєння ролей відповідно до правил системи.

Схема процесу

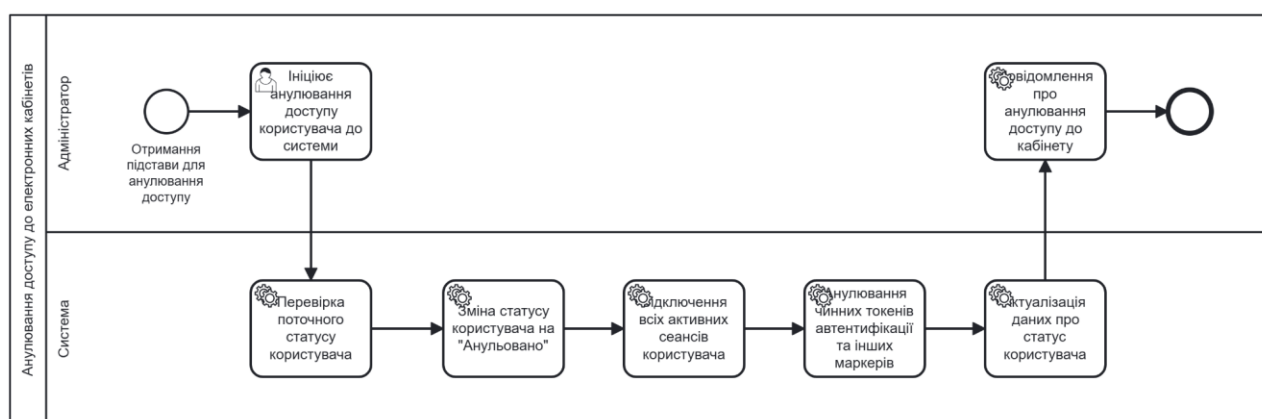


Схема бізнес-процесу. Анулювання доступу до електронних кабінетів

Передумови:

- Користувач зареєстрований у Системі та має підтверджений обліковий запис.
- У Системі існують адміністратори з підтвердженою роллю, які мають право ініціювати процедуру анулювання доступу.
- Наявна документально підтверджена підстава для анулювання доступу (офіційне повідомлення уповноваженого керівника або судове рішення, що набрало законної сили).

Опис процесу:

- Адміністратор отримує підставу для анулювання доступу користувача до Електронного кабінету:
 - офіційне повідомлення керівника державного органу, місцевої держадміністрації (військової адміністрації), органу місцевого самоврядування або особи, яка його заміщує;
 - судове рішення, що набрало законної сили, про необхідність анулювання доступу користувача.
- Адміністратор ініціює анулювання доступу користувача в Системі.
- Система виконує автоматичні дії з виконання анулювання:
 - перевіряє поточний статус користувача;
 - змінює статус на "Анульовано", що унеможлиблює подальше відновлення доступу без повторної реєстрації;
 - відключає всі активні сесии користувача;
 - анулює чинні токени автентифікації та інші маркери доступу.
 - актуалізує дані про статус користувача у всіх внутрішніх модулях
 - повертає до інтерфейсу базового облікового запису за умови звернення до заблокованого кабінету.
- Система формує повідомлення про анулювання доступу до Електронного кабінету, із зазначенням причини.

Бізнес-правила:

1. Анулювання доступу може виконувати лише користувач із підтвердженою роллю адміністратора.

2. Анулювання доступу здійснюється виключно на підставі офіційного повідомлення керівника уповноваженого органу або судового рішення, що набрало законної сили.
3. Після анулювання доступу користувача його обліковий запис переходить у статус «Анульовано» та не може бути відновлений.
4. Система повинна автоматично завершити всі активні сеанси користувача та анулювати чинні токени автентифікації.

Результат бізнес-процесу: Доступ користувача до Електронного кабінету анульовано. Система зафіксувала підставу анулювання, ініціатора процедури та оновлений статус користувача.

5.15.5.2.3. br-08. Автоматичне анулювання доступу до електронного кабінету

Основні відомості. Даний бізнес-процес визначає послідовність дій системи щодо автоматичного анулювання доступу користувача до Електронного кабінету. Автоматичне анулювання відбувається без участі адміністратора на підставі отримання системою інформації з державних електронних інформаційних ресурсів.

Схема процесу

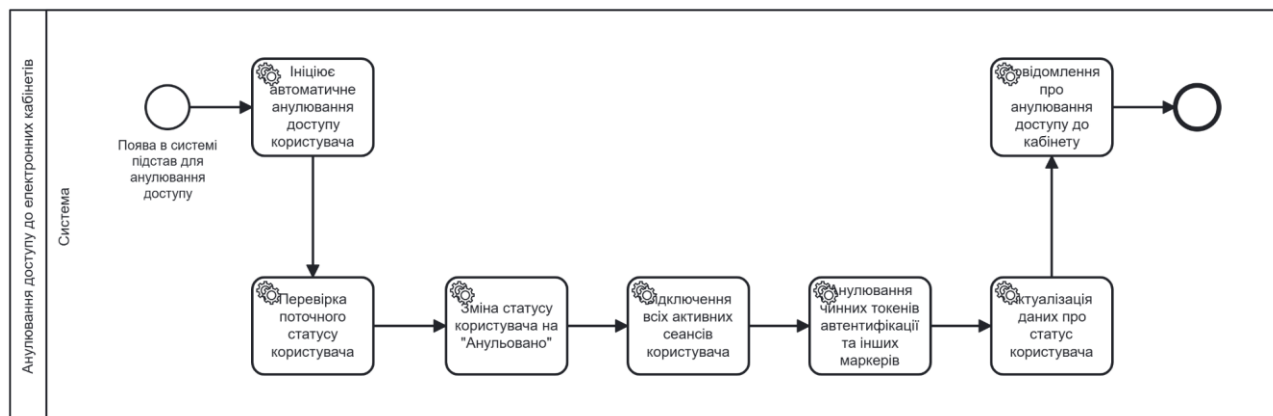


Схема бізнес-процесу. Автоматичне анулювання доступу до електронних кабінетів

camunda

<https://modeler.camunda.io/share/2b2e14ac-5e5e-4d89-b675-3c0741354852>

Передумови:

- Користувач зареєстрований у Системі та має підтверджений обліковий запис.

- Система інтегрована з державними електронними інформаційними ресурсами (ЄДР, реєстр ФОП, реєстр актів цивільного стану тощо) та підтримує регулярний або подієвий обмін даними.
- У Системі реалізований механізм перевірки чинності правового статусу користувача та його відповідності умовам доступу.

Опис процесу:

- а. Система у режимі реального часу або за розкладом перевіряє дані користувачів через електронну інформаційну взаємодію з державними реєстрами.
- б. Система отримує дані з одного або кількох державних електронних інформаційних ресурсів про настання підстав для анулювання доступу, зокрема:
 - втрату користувачем правового статусу або функцій, які визначають його право доступу до кабінету;
 - державну реєстрацію припинення юридичної особи
- в. У разі отримання підтвердженої інформації Система автоматично запускає процес:
 - перевіряє поточний статус користувача;
 - змінює статус на "Анульовано";
 - відключає всі активні сесії користувача;
 - анулює чинні токени автентифікації та інші маркери доступу.
 - актуалізує дані про статус користувача у всіх внутрішніх модулях
- г. Система формує повідомлення про анулювання доступу до Електронного кабінету, із зазначенням причини.

Бізнес-правила:

1. Автоматичне анулювання доступу виконується системою без участі адміністратора.
2. Підставою для анулювання є інформація, отримана з державних електронних інформаційних ресурсів.
3. Після анулювання доступу користувача його обліковий запис переходить у статус «Анульовано» та не може бути відновлений.

4. Повторне надання доступу можливе лише шляхом нової реєстрації користувача та проходження повної процедури автентифікації та авторизації.
5. Система повинна автоматично завершити всі активні сеанси користувача та анулювати чинні токени автентифікації.

Результат бізнес-процесу: Доступ користувача до Електронного кабінету анульовано. Система зафіксувала підставу анулювання, ініціатора процедури та оновлений статус користувача.

5.15.5.2.4. бр-09. Відновлення доступу до електронних кабінетів

Основні відомості. Даний бізнес-процес визначає послідовність дій адміністратора та системи щодо відновлення доступу користувача електронного кабінету, який був заблокований, після усунення підстав для блокування.

Схема процесу

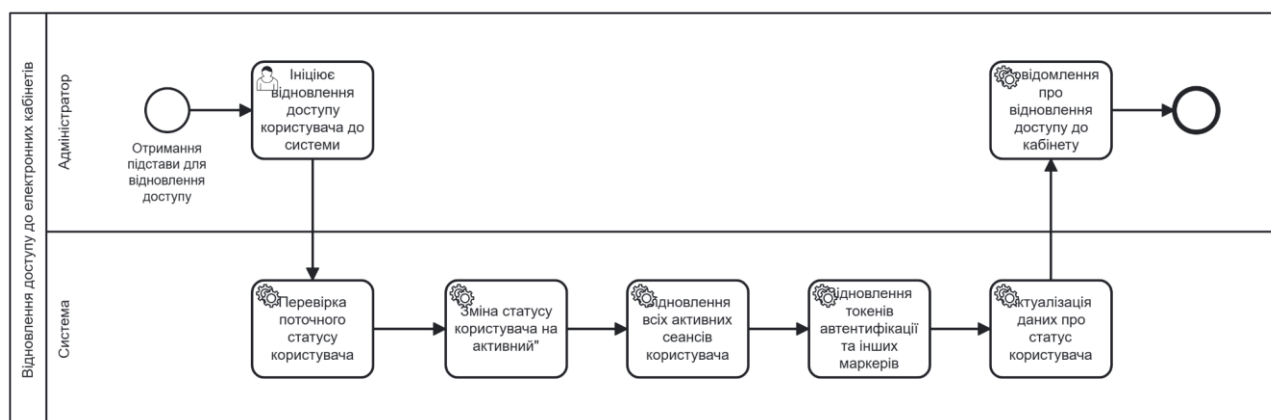


Схема бізнес-процесу. Відновлення доступу до електронних кабінетів

camunda

<https://modeler.camunda.io/share/61875c97-38a1-41b2-a90d-7593fd9ddb5f5>

Передумови:

- Користувач має зареєстрований обліковий запис у системі, який перебуває у статусі «Заблоковано».
- Адміністратор має роль та права для виконання дій з відновлення доступу.

- Наявна документально підтверджена підстава для відновлення доступу (офіційне повідомлення уповноваженого керівника або судове рішення, що набрало законної сили).

Опис процесу:

- Адміністратор отримує підставу для відновлення доступу користувача до Електронного кабінету:
 - повідомлення керівника державного органу, місцевої держадміністрації (військової адміністрації), органу місцевого самоврядування або особи, яка його заміщує, про припинення обставин, що стали підставою для блокування доступу; судове рішення, що набрало законної сили, про скасування блокування доступу користувача.
- Адміністратор ініціює відновлення доступу користувача в Системі.
- Система виконує автоматичні дії з виконання відновлення доступу:
 - перевіряє поточний статус користувача;
 - змінює статус на активний;
 - відновлює всі активні сеанси користувача;
 - відновлює токени автентифікації та інші маркери доступу.
 - актуалізує дані про статус користувача у всіх внутрішніх модулях
- Система формує повідомлення для користувача про відновлення доступу до Електронного кабінету.

Бізнес-правила:

- Відновлення доступу виконується лише за ініціативою адміністратора після усунення підстав для блокування.
- Система перевіряє поточний статус користувача перед відновленням доступу.
- Статус користувача після відновлення змінюється на активний.
- Усі попередні сесії та токени автентифікації залишаються недійсними. Після повторної автентифікації створюються нові токени доступу та ініціюються нові сеанси роботи.
- Користувач після відновлення отримує повідомлення про успішне надання доступу.

Результат бізнес-процесу: Доступ користувача до Електронного кабінету відновлено. Система зафіксувала підставу відновлення, ініціатора процедури, дату та час відновлення доступу та оновлений статус користувача.

5.15.5.3. Робота з відомостями про координаційну комісію/комісію з обстеження

5.15.5.3.1. br-11. Внесення в систему відомостей про уповноважених осіб місцевих державних (військових) адміністрацій

Основні відомості. Даний бізнес-процес описує послідовність дій для внесення в систему відомостей про уповноважених осіб місцевих державних (військових) адміністрацій, які будуть вносити в Систему відомості (дані) про склад координаційних комісій та комісій з обстеження, визначати відповідні ролі членів таких комісій.

Схема процесу

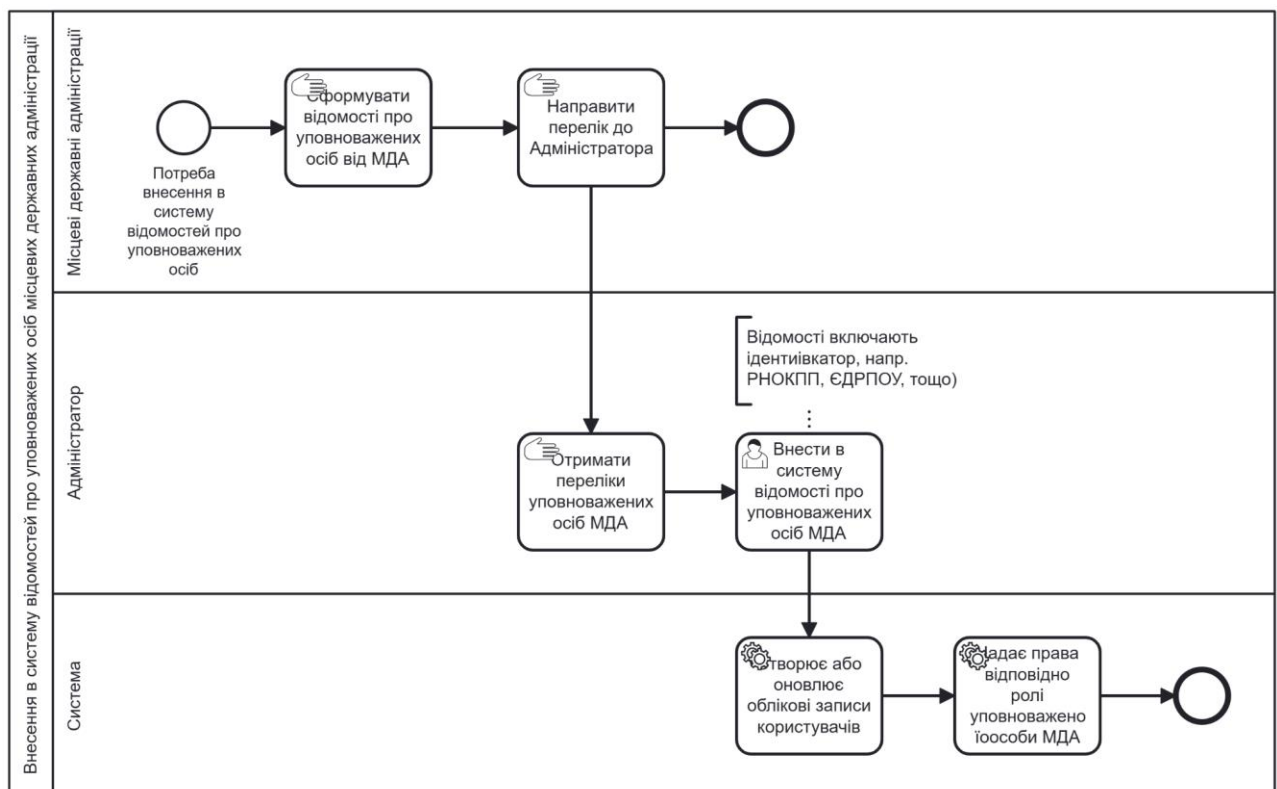


Схема бізнес-процесу. Внесення в систему відомостей про уповноважених осіб місцевих державних (військових) адміністрацій

Передумови:

- Місцеві державні (військові) адміністрації надали відомості організацій (для юридичних осіб) та реквізитів уповноважених осіб (ЄДРПОУ, РНОКПП тощо).
- Уповноважені особи МДА/МВА мають діючий електронний підпис (КЕП або УЕП).

Опис процесу:

- Адміністратор отримує від адміністрацій відомості про уповноважених осіб на роботу з відомостями про відповідні комісії в системі (напр. РНОКПП, ЄДРПОУ, посаду та іншу інформацію).
- Адміністратор вносить до системи відомості про таких осіб з призначенням відповідної ролі в системі.
- Система перевіряє внесені дані, актуалізує відомості та роль уповноваженої особи. Якщо користувач ще не проходив автентифікацію, такі дані зберігаються, а обліковий запис створюється автоматично під час першого входу.
- Уповноважені особи отримують доступ до відповідного Електронного кабінету.

Бізнес-правила:

- Внесення відомостей можливе лише на підставі офіційних даних від адміністрацій.

Примітка. Можливим альтернативним підходом, який доцільно розглянути при розробленні ТЗ, є автоматизоване надання ролі уповноваженої особи без попереднього ручного внесення даних адміністратором. У цьому варіанті в систему первинно вносяться лише ідентифікаційні дані організації (ЄДРПОУ) відповідної МДА/МВА.

Під час першої авторизації користувача, який підтверджує свою особу за допомогою електронного підпису, Система автоматично звіряє його ідентифікаційні дані з відомостями ЄДР. Якщо такий користувач визначений як керівник або керівник з обмеженнями відповідної організації, Система присвоює йому роль уповноваженої особи МДА/МВА без участі адміністратора. Примітка. Можливим альтернативним підходом, який доцільно розглянути при розробленні ТЗ, є автоматизоване надання

ролі уповноваженої особи без попереднього ручного внесення даних адміністратором. У цьому варіанті в систему первинно вносяться лише ідентифікаційні дані організації (ЄДРПОУ) відповідної МДА/МВА.

Під час першої авторизації користувача, який підтверджує свою особу за допомогою електронного підпису, Система автоматично звіряє його ідентифікаційні дані з відомостями ЄДР. Якщо такий користувач визначений як керівник або керівник з обмеженнями відповідної організації, Система присвоює йому роль уповноваженої особи МДА/МВА без участі адміністратора.

Результат бізнес-процесу. Відомості про уповноважених осіб внесено до системи, вони отримали відповідні ролі та доступ до Електронного кабінету для управління складом комісії/перегляду інформаційних та статистичних даних.

5.15.5.3.2. br-12. Додавання відомостей про координаційну комісію/комісію з обмеження

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою внесення в систему відомостей про відповідну координаційну комісію та/або комісію з обмеження та її членів, яка є релевантною для цілей функціонування даної системи.

Схема процесу

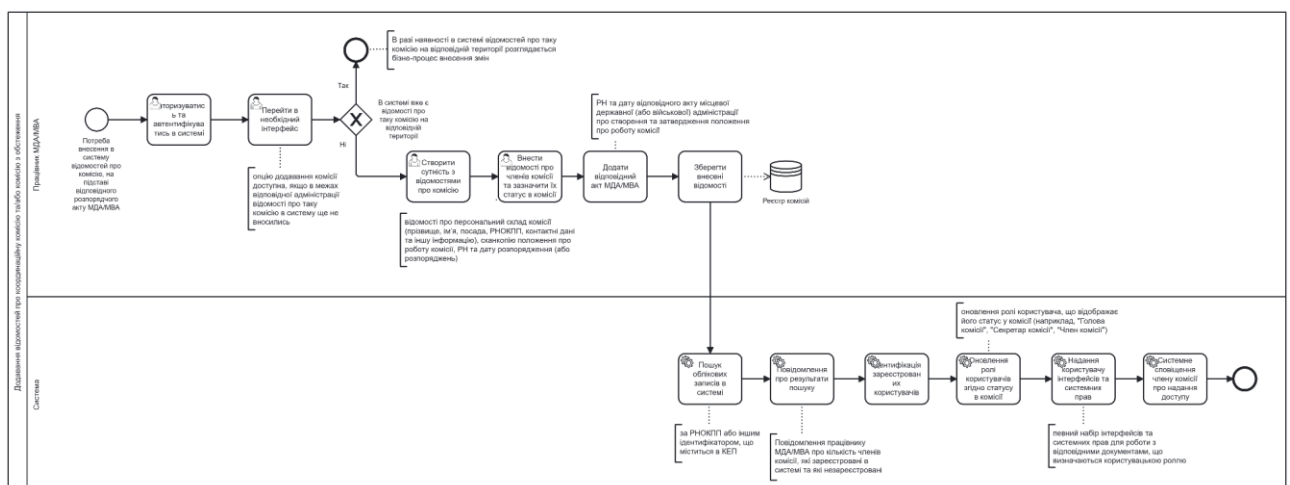


Схема бізнес-процесу. Додавання відомостей про координаційну комісію та/або комісію з обстеження

camunda

<https://modeler.camunda.io/share/3eeb4282-24cd-456c-bcbo-40309b5fae19>

Передумови:

- Уповноважена особа МДА/МВА авторизована та автентифікована в Системі та має права для внесення даних про комісію.
- Відомості про комісію ще не внесені до Системи для відповідної адміністрації.

Опис процесу:

- а. Уповноважена особа МДА/МВА автентифікується та авторизується в Системі як користувач з відповідною роллю та здійснює навігацію в необхідний розділ меню.
- б. Уповноважена особа МДА/МВА вибирає опцію додавання комісії (дана функція доступна, якщо в межах відповідної адміністрації відомості про таку комісію в систему ще не вносились) та переходить у відповідну форму.
- в. Уповноважена особа МДА/МВА вибирає опцію додавання відомостей про учасників відповідної комісії та вводить їх ПІБ, посаду, РНОКПП або інший ідентифікатор, що міститься в КЕП, контактні дані та інші відомості. Вказує роль нового члена в комісії (наприклад, "Голова комісії", "Секретар комісії", "Член комісії").
- г. Уповноважена особа МДА/МВА вносить реєстраційний номер (РН) та дату відповідного акту місцевої державної (або військової) адміністрації про створення та затвердження положення про роботу комісії, завантажує сканкопію, зберігає відомості та підписує ЕП.
- д. Система аналізує персональний склад комісії для подальшої ідентифікації користувачів та виконує пошук відповідних облікових записів в Системі. Для незареєстрованих членів, на момент внесення відомостей про склад комісії, застосовується процес відкладеної авторизації.
- е. Система ідентифікує відповідного члена комісії, зареєстрованого в системі за його РНОКПП або номером паспорту, що міститься в ЕП,

оновлює роль та відображає його статус у комісії (наприклад, "Голова комісії", "Секретар комісії", "Член комісії").

- g. Після успішної аутентифікації користувача, система використовує користувацьку роль, присвоєну ідентифікованому члену комісії (та збережену, наприклад, у сесії або токени), для надання дозволів на виконання операцій з документами та визначення доступних інтерфейсів Електронного кабінету. У випадку зміни ролей користувача, його поточна сесія або токен будуть інвалідовані, що вимагатиме повторного входу для оновлення системних прав.

Бізнес-правила:

1. Внесення відомостей здійснюється лише уповноваженою особою МДА/МВА з відповідною роллю та правами.
2. Для незареєстрованих членів комісії застосовується процес відкладеної авторизації.
3. Зміна ролей користувачів не вимагає повторного входу для оновлення системних прав.

Результат бізнес-процесу: Відомості про відповідну комісію успішно внесені в систему, члени комісії (в разі реєстрації в системі) отримали певну користувацьку роль та системні права для роботи з інтерфейсами та документами.

5.15.5.3.3. бр-13. Внесення відомостей про зміни до складу координаційної комісії/комісії з обстеження

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою внесення в систему відомостей про зміни в персональному складі відповідної координаційної комісії та/або комісії з обстеження.

Схема процесу

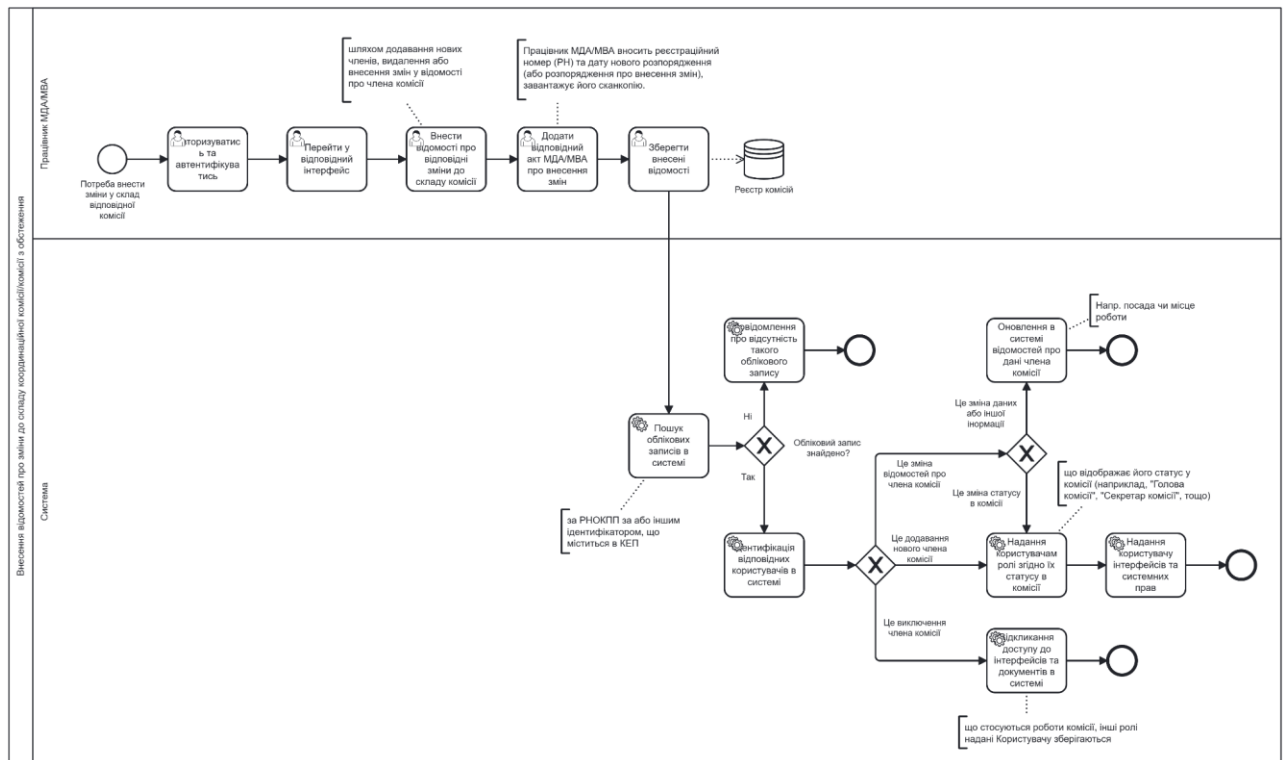


Схема бізнес-процесу. Внесення відомостей про зміни до складу координаційної комісії та/або комісії з обстеження.

camunda

<https://modeler.camunda.io/share/eb55dd8f-9454-41d3-b186-22108fe956cb>

Передумови:

- Уповноважена особа МДА/МБА має зареєстрований обліковий запис у системі та відповідну роль.
- В Системі створена відповідна комісія, склад якої підлягає оновленню.

Опис процесу:

- Уповноважена особа МДА/МБА автентифікується та авторизується в Системі як користувач з відповідною роллю та здійснює навігацію в необхідний розділ меню.
- Уповноважена особа МДА/МБА обирає опцію внесення змін до складу комісії та переходить у відповідну форму.
- (Альтернативний крок). Уповноважена особа МДА/МБА обирає опцію додавання нового члена комісії. Вводить ПІБ, посаду, РНОКПП або інший ідентифікатор, що міститься в КЕП, контактні

дані та інші відомості. Вказує роль нового члена в комісії (наприклад, "Голова комісії", "Секретар комісії", "Член комісії").

- d. (Альтернативний крок). Уповноважена особа МДА/МВА обирає члена комісії, якого необхідно виключити зі складу комісії та натискає відповідну опцію.
- e. (Альтернативний крок). Уповноважена особа МДА/МВА обирає члена комісії, відомості про якого необхідно змінити. Обирає опцію внесення змін та редагує відповідні поля (наприклад, посада, контактні дані, роль у комісії).
- f. Уповноважена особа МДА/МВА вносить реєстраційний номер (РН) та дату нового розпорядження (або розпорядження про внесення змін), завантажує його сканкопію, обирає опцію збереження та підписання внесених відомостей.
- g. Система автоматично аналізує зміни в персональному складі комісії, здійснює пошук відповідних облікових записів та оновлює відомості про склад комісії в базі даних.
- h. Система ідентифікує відповідного користувача, зареєстрованого в системі, оновлює відомості та/або його роль, що відображає його новий статус у комісії (наприклад, "Голова комісії", "Секретар комісії", "Член комісії"). Для виключених членів комісії система відкликає доступ до інтерфейсів та документів, пов'язаних з роботою цієї комісії та надсилає повідомлення на електронну пошту, якщо вона була зазначена в контактних даних.
- i. Після успішної аутентифікації користувача, система використовує користувацьку роль, присвоєну ідентифікованому члену комісії (та збережену, наприклад, у сесії або токени), для надання дозволів на виконання операцій з документами та визначення доступних інтерфейсів Електронного кабінету.
- j. Система надсилає всім членам комісії автоматичні інформаційні сповіщення про новий склад комісії. В разі відсутності в системі відповідного облікового запису, повідомлення направляються на електронні адреси, якщо вони були зазначені у відомостях про члена комісії.

Бізнес-правила:

1. Внесення змін у персональний склад координаційної комісії може здійснювати лише уповноважена особа МДА/МБА з відповідною роллю в системі.
2. Всі зміни вносяться на підставі офіційного розпорядження або іншого документа адміністрації.
3. Виключення членів комісії автоматично відкликає їх доступ до пов'язаних інтерфейсів та документів.
4. Система повинна інформувати всіх членів комісії про внесені зміни.

Результат бізнес-процесу: Відомості про зміни до персонального складу відповідної комісії успішно внесені в систему, члени комісії (в разі реєстрації в системі) отримали (оновили або втратили) певні системні права для роботи з інтерфейсами та документами.

5.15.5.4. Робота з відомостями про Тимчасову робочу групу координаційної комісії/комісії з обстеження

5.15.5.4.1. br-15. Додавання відомостей про Тимчасову робочу групу координаційної комісії/комісії з обстеження

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою внесення в систему відомостей про персональний склад учасників ТРГ, їх ролі в системі. Учасники ТРГ можуть отримувати права для роботи з інтерфейсами та документами (напр. додавати ОНМ в систему) з урахуванням принципу територіальності повноважень. Початкові територіальні повноваження за замовчанням мають наслідуватися від повноважень комісії і не мають виходити за територію діяльності відповідної комісії.

Схема процесу

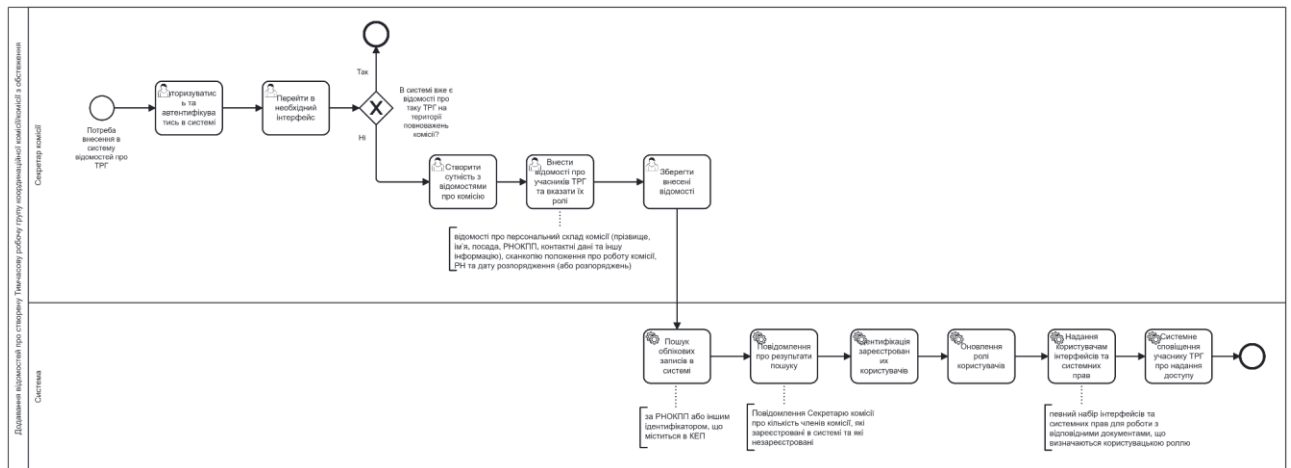


Схема бізнес-процесу. Внесення відомостей про Тимчасову робочу групу координаційної комісії/комісії з обстеження

camunda

<https://modeler.camunda.io/share/1abd11e1-574d-43cc-af26-8be4e41c19a6>

Передумови:

- Відповідна комісія ухвалила рішення про створення Тимчасової робочої групи

Опис процесу:

- Відповідна комісія на засіданні (поза системою) приймає рішення про утворення ТРГ.
- Секретар комісії автентифікується та авторизується в системі як користувач з відповідною роллю та здійснює навігацію в необхідний розділ меню (інтерфейс).
- Секретар комісії обирає опцію внесення відомостей про ТРГ та переходить у відповідну форму.
- Секретар комісії обирає опцію додавання нового учасника ТРГ, вводить ПІБ, посаду, РНОКПП або номер паспорту, що міститься в КЕП, контактні дані та інші відомості. Вказує роль учасника робочої групи, з доступного для ТРГ переліку ролей, яка надається користувачу в межах повноважень відповідної МДА.
- Секретар комісії вибирає опцію збереження внесених відомостей.
- Система автоматично аналізує внесений персональний склад ТРГ для подальшої ідентифікації користувачів та виконує пошук

відповідних облікових записів в системі.

- g. Система ідентифікує відповідного користувача, попередньо зареєстрованого в системі за його РНОКПП або номером паспорту, що міститься в КЕП, та оновлює роль, що відображає його статус у ТРГ.
- h. Після успішної аутентифікації користувача, Система використовує користувацьку роль, присвоєну ідентифікованому члену комісії (та збережену, наприклад, у сесії або токєні), для надання дозволів на виконання операцій з документами та визначення доступних інтерфейсів Електронного кабінету. У випадку зміни ролей користувача, його поточна сесія або токєн будуть інвалідовані, що вимагатиме повторного входу для оновлення системних прав.

Бізнес-правила:

- 1. Внесення відомостей здійснюється лише уповноваженими користувачами (головою, секретарем комісії або особами з відповідною роллю).
- 2. Ролі та територіальні повноваження учасників ТРГ не можуть виходити за межі повноважень відповідної комісії.

Результат бізнес-процесу: Відомості про склад відповідної ТРГ успішно внесені в систему, учасники отримали певні системні права для роботи з інтерфейсами та документами.

5.15.5.4.2. бр-16. Внесення змін до складу Тимчасової робочої групи координаційної комісії/комісії з обстеження

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою внесення в систему відомостей про персональний склад учасників ТРГ, їх ролі в системі. Учасники ТРГ можуть отримувати права для роботи з інтерфейсами та документами (напр. додавати ОНМ в систему) з урахуванням принципу територіальності повноважень. Початкові територіальні повноваження за замовчанням мають наслідуватися від повноважень комісії і не мають виходити за територію діяльності відповідної комісії.

Схема процесу

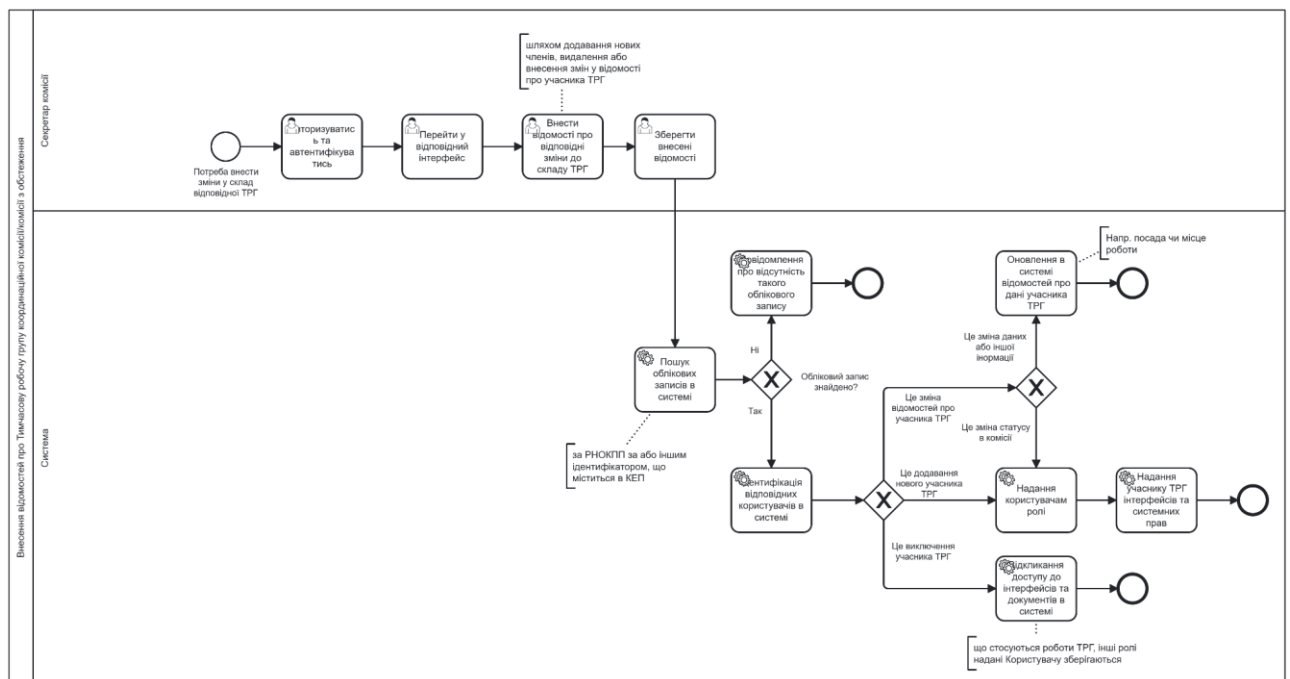


Схема бізнес-процесу. Внесення відомостей про Тимчасову робочу групу координаційної комісії/комісії з обстеження

camunda

<https://modeler.camunda.io/share/5d23fcbe-3ffe-4183-bbb9-da557eb7365e>

Передумови:

- Секретар відповідної комісії має зареєстрований обліковий запис у системі та відповідну роль.
- В системі створена відповідно ТРГ, склад якої підлягає оновленню.

Опис процесу:

- а. Секретар комісії автентифікується та авторизується в системі як

користувач з відповідною роллю та здійснює навігацію в необхідний розділ меню.

- b. Секретар комісії обирає опцію внесення змін до складу комісії та переходить у відповідну форму.
- c. Секретар комісії обирає опцію додавання нового учасника ТРГ. Вводить ПІБ, посаду, РНОКПП або інший ідентифікатор, що міститься в КЕП, контактні дані та інші відомості (в разі необхідності). Вказує роль нового учасника.
- d. (Альтернативний крок). Секретар комісії обирає учасника ТРГ, якого необхідно виключити зі складу групи та натискає відповідну опцію.
- e. (Альтернативний крок). Секретар комісії обирає учасника ТРГ, відомості про якого необхідно змінити. Обирає опцію внесення змін та редагує відповідні поля (наприклад, посада, контактні дані, роль у комісії).
- f. Система автоматично аналізує зміни в персональному складі ТРГ, здійснює пошук відповідних облікових записів та оновлює відомості про склад комісії в базі даних.
- g. Система ідентифікує відповідного користувача, зареєстрованого в системі, оновлює відомості та/або його роль, що відображає його новий статус в ТРГ. Для виключених учасників ТРГ система відкликає доступ до інтерфейсів та документів, пов'язаних з роботою цієї ТРГ.
- h. Після успішної аутентифікації користувача, система використовує користувацьку роль, присвоєну ідентифікованому учаснику ТРГ (та збережену, наприклад, у сесії або токени), для надання дозволів на виконання операцій з документами та визначення доступних інтерфейсів Електронного кабінету. У випадку зміни ролей користувача, його поточна сесія або токен будуть інвалідовані, що вимагатиме повторного входу для оновлення системних прав.
- i. Система надсилає всім учасникам ТРГ автоматичні інформаційні сповіщення про новий склад. В разі відсутності в системі відповідного облікового запису, повідомлення направляються на електронні адреси, якщо вони були зазначені у відомостях про

учасника ТРГ.

Бізнес-правила:

1. Внесення змін у персональний склад ТРГ може здійснювати лише секретар комісії з відповідною роллю в системі.
2. Всі зміни вносяться на підставі офіційного розпорядження або іншого документа адміністрації.
3. Внесені відомості мають відображати актуальні ролі та статуси учасників ТРГ.
4. Виключення учасників ТРГ автоматично відкликає їх доступ до пов'язаних інтерфейсів та документів.
5. Система повинна інформувати всіх учасників ТРГ про внесені зміни.

Результат бізнес-процесу: Відомості про зміни до персонального складу ТРГ успішно внесені в систему, учасники робочої групи отримали (або втратили) певні системні права для роботи з інтерфейсами та документами.

5.15.5.5. Робота зі здійснення обліку ОНМ

5.15.5.5.1. br-17. Внесення в систему відомостей про ОНМ

Основні відомості. Даний бізнес-процес описує послідовність дій, що виконуються з метою внесення до системи відомостей про ОНМ, що підлягають обстеженню в межах територіальних повноважень конкретної координаційної комісії.

Схема процесу

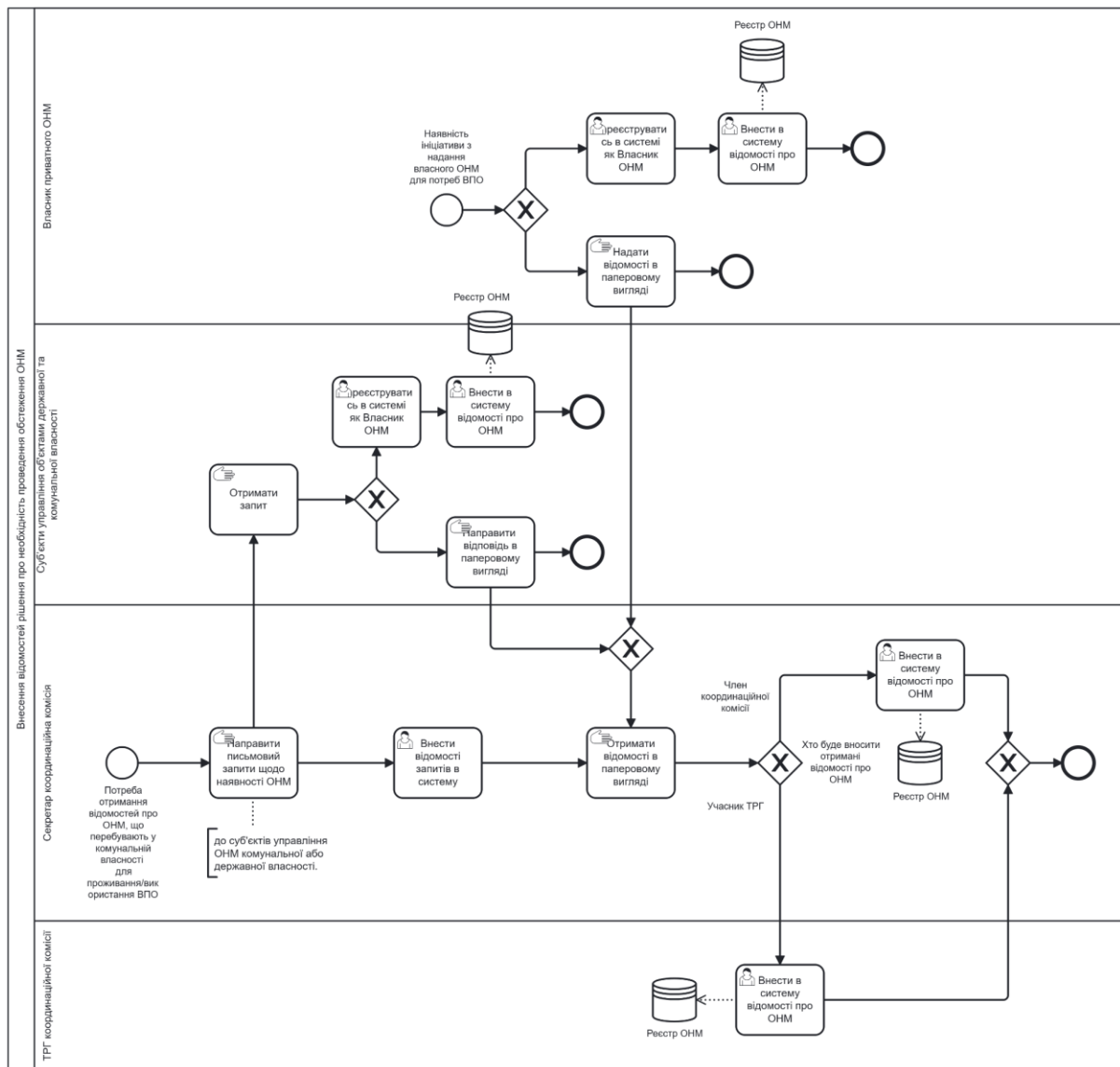


Схема бізнес-процесу. Внесення в систему відомостей про ОНМ

camunda

<https://modeler.camunda.io/share/1e863865-7ad5-43c4-8223-ac32582078f3>

Передумови:

- В Систему внесені відомості про координаційну комісію.
- ОНМ відомості про який вносяться територіально належить до повноважень цієї координаційної комісії.
- Відповідним членам координаційної комісії та/або учасникам ТРГ надано ролі, що дозволяють виконувати дії з внесення відомостей про ОНМ.

Опис подій:

- a. Координаційна комісія поза системою направляє письмові запити щодо отримання відомостей про ОНМ, які можуть перебувати у комунальній власності або державній власності.
- b. Власники ОНМ, що перебувають у приватній власності, за власною ініціативою поза системою можуть подати до координаційної комісії за місцем розташування об'єкта, відомості про такі ОНМ, зокрема, інформацію про місцезнаходження, призначення об'єкта та підтвердження права власності на нього.
- c. Координаційна комісія поза Системою отримує та опрацьовує інформацію про ОНМ, надану у відповідь на запити або подану власниками за власною ініціативою.
- d. Член координаційної комісії або учасник ТРГ, як користувач з відповідною роллю, створює сутність ОНМ та вносить в Систему отримані відомості про ОНМ, за формою цього документу (порядок внесення відомостей для ОНМ, що є земельними ділянками наведений в описі альтернативного процесу).

Альтернативні дії:

- a. Користувач на кроці d основного потоку у формі створення сутності ОНМ обирає тип ОНМ "Земельна ділянка".
- b. Система ініціює перевірку кадастрового номера у зовнішніх інтегрованих джерелах (ДЗК) для підтвердження існування об'єкта та відповідності формату номера.
- c. На цьому етапі система здійснює лише ідентифікацію (метчинг) кадастрового номера, після чого користувач вносить решту відомостей визначених відповідною формою вручну (адреса, площа, форма власності, цільове призначення тощо).
- d. Після збереження даних створена сутність земельної ділянки стає доступною для подальшої роботи в Системі.

Примітка. Власники ОНМ можуть автентифікуватись та авторизуватись в системі з відповідною роллю, та подати відомості про такі об'єкти самостійно - шляхом створення сутності ОНМ та зазначення необхідних відомостей, визначених формою цього документу.

Бізнес-правила:

1. ОНМ може бути внесений до Системи лише в межах територіальних повноважень координаційної комісії.
2. У разі, якщо об'єкт належить іншій адміністративно-територіальній одиниці, Система забороняє внесення даних.

Результат бізнес-процесу. До Системи внесено відомості про ОНМ, що належить до територіальних повноважень відповідної координаційної комісії. Статус таких ОНМ в Системі: “потребує верифікації (обстеження)”. Дані збережені та доступні для подальшої роботи в Системі.

5.15.5.5.2. бр-18. Внесення відомостей рішення про необхідність проведення обстеження ОНМ

Основні відомості. Даний бізнес-процес описує послідовність дій, що виконуються з метою внесення до системи відомостей рішення про проведення обстеження ОНМ.

Схема процесу

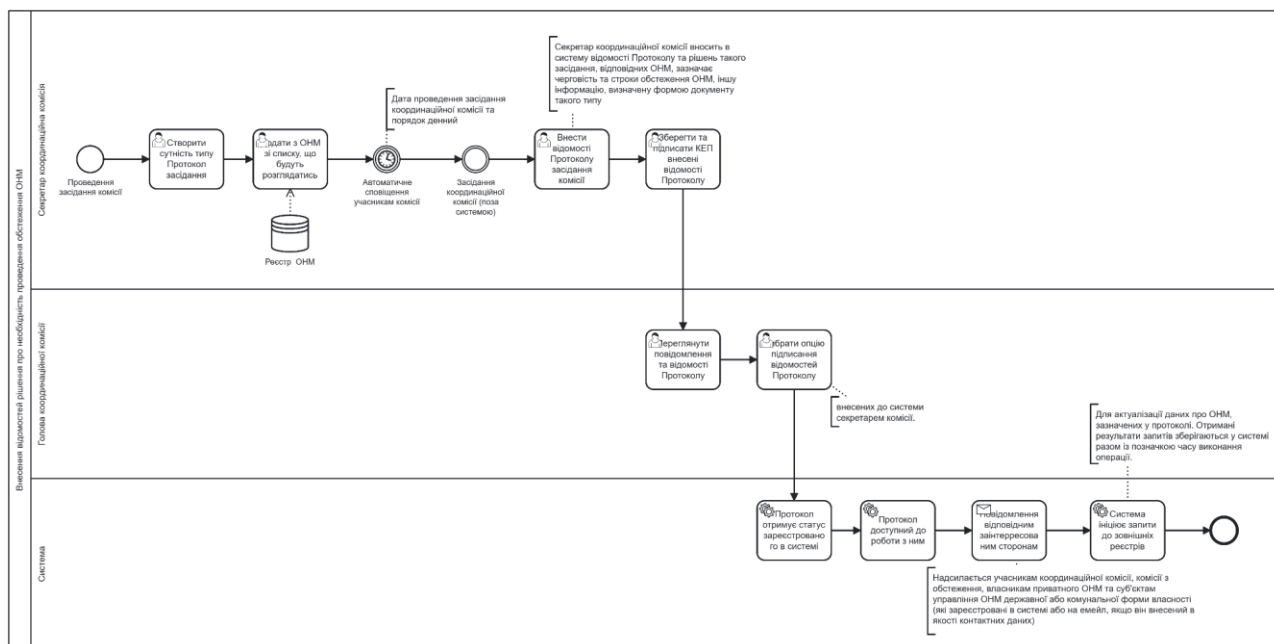


Схема бізнес-процесу. Внесення відомостей рішення про проведення обстеження ОНМ

camunda

<https://modeler.camunda.io/share/8deo2d9e-92a9-4481-97a6-631ad7oda156>

Передумови:

- Користувачі, що беруть участь у процесі, мають зареєстровані облікові записи та відповідні ролі в системі.
- У Систему несені відомості про ОНМ, що належать до територіальних повноважень відповідної координаційної комісії.

Опис подій:

- а. Секретар координаційної комісії за три дні до засідання, створює сутність Протоколу, в її складі формує порядок денний, додаючи ОНМ, що мають розглядатись на засіданні (з переліку ОНМ які були внесені до системи в межах територіальних повноважень комісії, але щодо яких відсутні акти обстеження, або зі статусом необхідності повторного обстеження чи неможливості використання).
- б. Члени координаційної комісії які зареєстровані в системі отримують сповіщення та ознайомлюються з відомостями про ОНМ, що мають обстежуватись (незареєстровані отримують повідомлення на e-mail, якщо він внесений в якості контактних даних).
- с. Відбувається засідання координаційної комісії (дія поза системою) де приймається рішення, в тому числі - про проведення обстеження ОНМ, із встановленням черговості та строків.
- д. Секретар координаційної комісії вносить в картку сутності Протоколу відомості рішень такого засідання, зазначає ОНМ, які підлягають обстеженню, зазначає черговість та строки обстеження, іншу інформацію, визначену формою документу такого типу, завантажує сканкопію протоколу засідання.
- е. Секретар координаційної комісії протягом 5 робочих днів з дня засідання підписує електронним підписом документ Протоколу, чим фіксує завершення процесу роботи з даним документом.
- ф. Голова комісії отримує відповідне повідомлення та після перегляду відомостей Протоколу підписує електронним підписом документ Протоколу.
- г. Після підписання протоколу засідання координаційної комісії Система автоматично ініціює запити до зовнішніх реєстрів, з якими реалізовано інтеграцію, для отримання даних про ОНМ, зазначених

у протоколі. Отримані результати запитів зберігаються у системі разом із позначкою часу виконання операції.

- h. Система автоматично формує повідомлення (сповіщення) відповідним учасникам координаційної комісії, відповідних комісій з обстеження, ТРГ (які зареєстровані в системі або на e-mail, якщо він внесений в якості контактних даних) про появу протоколу засідання координаційної комісії.

Бізнес-правила:

1. Сканкопія протоколу засідання повинна бути внесена секретарем до системи протягом 5 робочих днів після засідання.
2. Голова комісії та секретар підписує електронним підписом відомості Протоколу.
3. Сповіщення надсилаються всім зареєстрованим учасникам або на електронну пошту, якщо вона зазначена.

Примітка. Одним із можливих технічних рішень, яке може бути розглянуте під час розроблення ТЗ, є автоматичне додавання до чернетки протоколу засідання координаційної комісії ОНМ, попередньо внесених у Систему та щодо яких відсутні акти обстеження або зі статусом необхідності повторного обстеження чи неможливості використання.

Результат бізнес-процесу. Відомості протоколу засідання координаційної комісії внесені до системи, підписані головою та секретарем та містять відомості про ОНМ які підлягають обстеженню, черговість та строки їх обстеження, іншу інформацію

5.15.5.5.3. br-19. Внесення відомостей актів обстеження ОНМ

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою внесення до системи відомостей актів обстеження ОНМ, складених відповідними комісіями.

Схема процесу

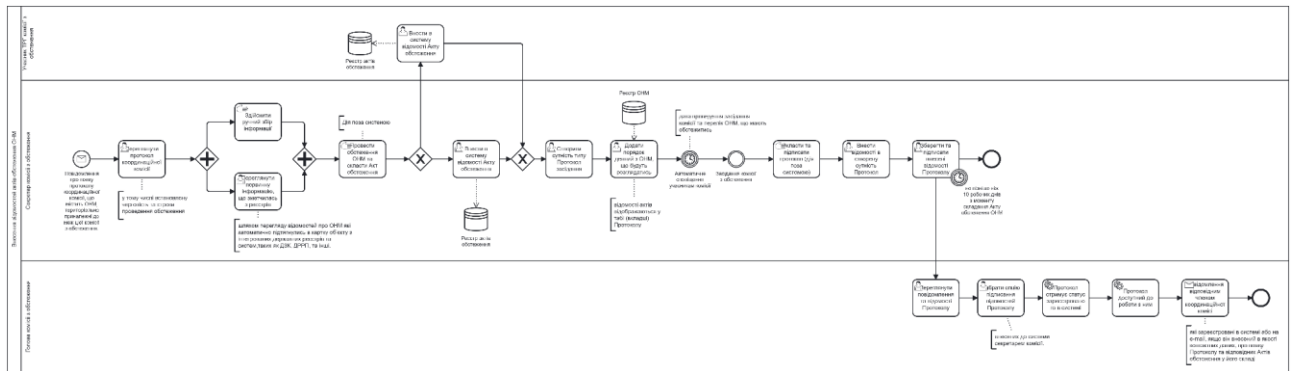


Схема бізнес-процесу. Внесення відомостей актів обстеження ОНМ

camunda

<https://modeler.camunda.io/share/267fff37-728b-46ab-94a5-449291eae35e>

Передумови:

- В Системі наявний Протокол координаційної комісії з переліком ОНМ, що підлягають обстеженню.

Опис процесу:

- Комісія з обстеження отримує повідомлення в Системі про появу протоколу координаційної комісії, що містить перелік ОНМ, територіально приналежних до відповідного району.
- Комісія з обстеження поза системою здійснює збір необхідної інформації про ОНМ, а також переглядає в Системі відомості про ОНМ які отримано через запит до інтегрованих реєстрів та державних систем в картці об'єкту (зокрема з ДЗК, ДРРП).
- Комісія з обстеження поза системою проводить обстеження ОНМ.
- Комісія з обстеження поза системою складає акт обстеження ОНМ який затверджується головою комісії з обстеження та підписується її членами і залученими особами.
- Секретар комісії, або учасник ТРГ з відповідною роллю додає в систему Акт обстеження ОНМ.
- Секретар комісії не пізніше ніж за три дні до засідання, створює документ типу Протокол, додає відомості про ОНМ, що були обстежені з відповідним Актом обстеження.
- Члени комісії які зареєстровані в системі отримують сповіщення та

ознайомлюються з відомостями ОНМ та відповідних Актів обстеження (незареєстровані отримують повідомлення на e-mail, якщо він внесений в якості контактних даних).

- h. Відбувається засідання комісії з обстеження (дія поза системою), за результатами якого складається відповідний протокол.
- i. Секретар комісії не пізніше ніж 10 робочих днів з дня складання Протоколу щодо затвердження акту обстеження вносить в картку документу відомості рішень такого засідання, заповнює відповідні поля щодо підсумкової (резолютивної) частини протоколу, вибирає опцію підписання внесених відомостей, чим фіксує завершення процесу роботи з даним документом.
- j. На підставі заповнених відомостей (даних) при підписанні протоколу комісії відомості (дані) щодо ОНМ з зазначенням статусу в частині можливості/неможливості використання ОНМ для проживання ВПО автоматично переносяться (доповнюються) та відображаються на публічній карті.
- k. Голова комісії отримує відповідне повідомлення та після перегляду відомостей Протоколу обирає опцію підписання відомостей Протоколу, внесених до системи секретарем комісії.
- l. Система автоматично формує повідомлення (сповіщення) відповідним членам координаційної комісії (які зареєстровані в системі або на e-mail, якщо він внесений в якості контактних даних) про появу Протоколу та відповідних Актів обстеження у його складі.

Бізнес-правила:

- 1. Внесення актів обстеження здійснюється лише авторизованим користувачем із відповідною роллю (секретар комісії або інший користувач).
- 2. Протокол та акти обстеження повинні бути внесені до системи у встановлені строки (10 робочих днів).
- 3. Голова комісії та секретар підписує відомості Протоколу в системі електронним підписом.
- 4. Сповіщення надсилаються зареєстрованим членам комісії або на e-mail, якщо він зазначений у контактних даних.

Результат бізнес-процесу. Відомості актів обстеження ОНМ внесені в систему, Протокол засідання комісії підписаний головою комісії та секретарем, а всі члени комісії отримали повідомлення про результати обстеження та висновки комісії.

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою розгляду координаційними комісіями актів обстеження ОНМ, складених відповідними комісіями з обстеження.

[illegible]

camunda

<https://modeler.camunda.io/share/b5e3b134-4516-49ec-b1b3-5d2b888bac52>

Передумови:

- Члени координаційної комісії зареєстровані в системі та мають відповідні ролі та права доступу. В системі створено та збережено Акти обстеження ОНМ, що потребують розгляду. Секретар комісії має права створення, редагування (до моменту підписання) та збереження картки Протоколів засідань.

Опис процесу:

- a. Секретар координаційної комісії за 3 дні до засідання, в системі створює документ типу Протоколу, в його складі формує порядок денний, додаючи ОНМ, що мають розглядатись на засіданні.
- b. Члени комісії (які зареєстровані в системі) отримують сповіщення та ознайомлюються з відомостями ОНМ та відповідних Актів обстеження, що виносяться на розгляд комісії.
- c. Координаційна комісія проводить засідання (дія поза системою), де розглядає визначений перелік актів обстеження.
- d. Секретар комісії (або інший авторизований користувач з відповідною користувацькою роллю) вносить в картку створеної сутності Протоколу відомості протоколу, завантажує його сканкопію. На цьому кроці також зазначається висновок комісії в форматі робочого статусу ОНМ за результатами обстеження (див. довідник).
- e. Секретар комісії вибирає опцію збереження та підписання внесених відомостей, чим фіксує завершення процесу роботи з даним документом.
- f. Голова комісії отримує відповідне повідомлення та після перегляду відомостей Протоколу обирає опцію підтвердження та підписання відомостей Протоколу, внесених до системи секретарем комісії.
- g. Система автоматично формує повідомлення (сповіщення) відповідним членам координаційної комісії (які зареєстровані в системі або на e-mail, якщо він внесений в якості контактних даних) про появу Протоколу та результатів розгляду Актів обстеження (та ОНМ) у його складі.
- h. Система автоматично відображає на публічному порталі відомості

про ОНМ які можуть бути використані для проживання ВПО.

- і. (Альтернативний крок). В разі прийняття рішення щодо доцільності проведення додаткового обстеження ОНМ такі об'єкти отримують відповідний статус та в подальшому підлягають повторному обстеженню комісіями. Включає дії щодо перегляду статусу таких об'єктів членами відповідної комісії з обстеження, складення Акту обстеження та повторний розгляд на засідання координаційної комісії.
- ї. (Альтернативний крок). В разі прийняття рішення щодо неможливості використання ОНМ такі об'єкти залишаються в системі з відповідним статусом. Координаційна комісія за потреби може їх заново розглянути згідно даного процесу та ініціювати повторне обстеження таких об'єктів.
- к. (Альтернативний крок). В разі прийняття координаційною комісією рішення щодо направлення акту на доопрацювання щодо такого ОНМ зазначається додатковий статус з приміткою щодо необхідності усунення недоліків з боку комісії з обстеження.

Довідник. d-01. Статуси ОНМ

№	Тип ОНМ	Значення статусу
1	Об'єкти нерухомого майна (квартири, житлові та нежитлові приміщення) та Об'єкти нерухомого майна (житлові будинки, будівлі, споруди (їх окремі частини))	можливе використання ОНМ для проживання ВПО
		неможливе використання ОНМ для проживання ВПО
		можливість використання ОНМ для проживання ВПО за умови проведення його реконструкції та/або переобладнання
		доцільність проведення додаткового обстеження ОНМ

2	Об'єкти нерухомого майна (земельні ділянки)	можливе використання земельної ділянки для будівництва ОНМ для проживання ВПО та/або розміщення ТС, їх комплексів, призначених для життєзабезпечення (тимчасового проживання та обслуговування) ВПО)
		неможливе використання земельної ділянки для будівництва ОНМ для проживання ВПО та/або розміщення ТС, їх комплексів, призначених для життєзабезпечення (тимчасового проживання та обслуговування) ВПО)
		необхідність вчинення дій для можливості використання земельної ділянки для будівництва ОНМ для проживання ВПО та/або розміщення ТС, їх комплексів, призначених для життєзабезпечення (тимчасового проживання та обслуговування) ВПО)

Бізнес-правила:

1. Протокол формується не пізніше ніж за три дні до засідання координаційної комісії.
2. Голова комісії та секретар підписує електронним підписом відомості Протоколу.
3. Публікація відомостей про ОНМ на публічному порталі здійснюється автоматично після підтвердження Протоколу.

Результат бізнес-процесу: Відомості Протоколу засідання комісії внесено в систему, члени координаційної комісії які зареєстровані в системі отримали сповіщення, відомості про ОНМ отримують статус згідно довідників та каталогів системи, зокрема, але не виключно: можливе використання ОНМ для проживання ВПО; потребує додаткового обстеження або непридатний зберігаються в системі для подальшої роботи з зазначенням щодо всіх статусів ОНМ: станом на (з зазначенням дати протоколу засідання координаційної комісії, назви координаційної комісії та його номеру).

5.15.5.6. Робота з матеріалами роботи комісій, які були складені до моменту запуску системи

5.15.5.6.1. br-21. Внесення матеріалів роботи комісії, які були складені до моменту запуску системи

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою забезпечення процесу внесення матеріалів роботи комісії, зокрема протоколів засідань, актів обстеження та інших релевантних документів, які були складені та оформлені до моменту запуску системи.

Схема процесу

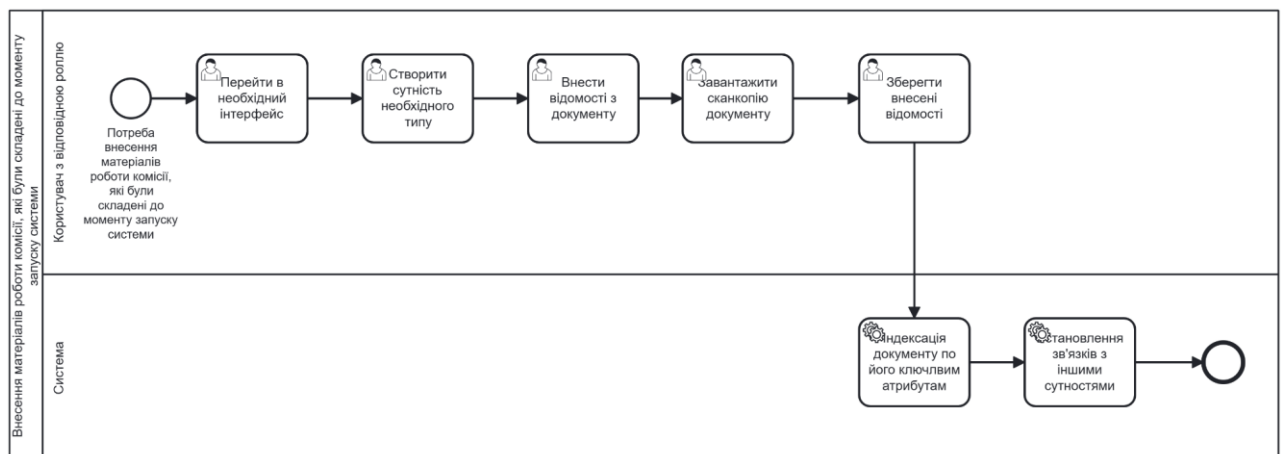


Схема бізнес-процесу. Внесення матеріалів роботи комісії, які були складені до моменту запуску системи

Передумови:

- Користувач автентифікований та авторизований у системі з роллю, що надає доступ до внесення матеріалів роботи координаційної комісії та/або комісії з обстеження.
- Документи доступні в сканованому вигляді для завантаження в Систему.

Опис процесу:

- а. Користувач автентифікується та авторизується в системі з відповідною роллю та здійснює навігацію в необхідний розділ меню (інтерфейс).
- б. Користувач обирає опцію внесення матеріалів роботи комісії, які були складені до моменту запуску системи.
- в. Користувач створює в системі сутність необхідного типу та вносить відомості документу, який був складений до моменту запуску системи, зокрема завантажує його сканкопію.
- г. Користувач вибирає опцію збереження внесених відомостей, що засвідчує факт внесення інформації уповноваженою особою та відповідність завантажених даних паперовому оригіналу.
- д. Система індексує документ по ключових атрибутах (тип документа, дата, номер, пов'язана комісія). За цими атрибутами він стає доступним у пошуку, роблячи його доступним для пошуку та перегляду у системі.

Бізнес-правила:

1. Внесення матеріалів здійснюється лише уповноваженими користувачами з відповідними ролями.

Результат бізнес-процесу: Документи роботи комісій (протоколи, акти обстеження, тощо), які були створені до запуску Системи, успішно внесені до системи та інтегровані в єдину інформаційну базу. Це забезпечує повноту даних, можливість їх подальшого використання для аналізу, пошуку та підтримки актуальності інформації про житловий фонд для ВПО.

5.15.5.7. Робота неавторизованого користувача з порталом

5.15.5.7.1. br-22. Робота неавторизованого користувача з порталом

Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою забезпечення доступу для широкого кола користувачів (в першу чергу, самих ВПО, а також громадськості, волонтерів тощо) до актуальних публічних відомостей про ОНМ.

Схема процесу

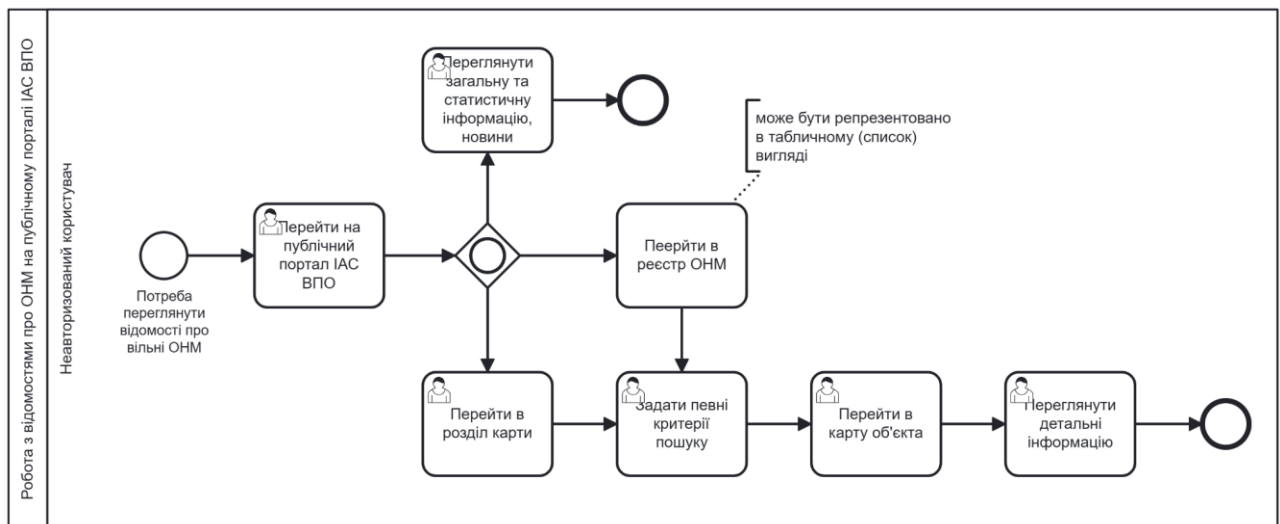


Схема бізнес-процесу. Робота неавторизованого користувача з порталом

camunda

<https://modeler.camunda.io/share/3d8983e3-8e28-43bd-b6de-1239cfc028d5>

Опис процесу:

- Неавторизований користувач здійснює перехід на головну сторінку публічного порталу Системи.
- Публічний портал завантажує та відображає головну сторінку, що містить пошукову форму, фільтри, загальну статистику та карту.
- Неавторизований користувач публічного порталу вводить критерії пошуку (наприклад, область, населений пункт, тип об'єкта, кількість

місць, статус ОНМ згідно довідників та каталогів Системи) або застосовує фільтри для звуження вибірки об'єктів.

- d. Публічний портал формує запит до бази даних (відповідних реєстрів) системи на отримання інформації, що відповідає запиту користувача.
- e. Система (або портал) обробляє запит, вибирає релевантні та дозволені до публічного відображення дані.
- f. Публічний портал отримує результати та відображає їх неавторизованому користувачеві у зручному форматі (список, таблиця, точки на карті).
- g. Неавторизований користувач публічного порталу може обрати конкретний об'єкт зі списку результатів, щоб переглянути його детальний опис (характеристики, потреби у ремонті, фотографії, історію статусу – в межах публічної інформації).
- h. Публічний портал відображає відомості (дані) щодо ОНМ, що є публічною інформацією.
- i. Неавторизований користувач публічного порталу аналізує отриману інформацію, можливо, повертається до списку, змінює критерії пошуку або завершує роботу з порталом.
- j. (Альтернативний крок) Користувач публічного порталу може переглядати аналітичні розділи порталу, що містять агреговані статистичні дані та звіти щодо обліку та використання ОНМ для ВПО.

Бізнес-правила:

- 1. Дані повинні бути актуальними та оновлюватися динамічно, відповідно до змін у внутрішній базі системи.
- 2. Пошук та перегляд інформації на публічному порталі доступні без авторизації.
- 3. Неавторизований Користувач може переглядати тільки публічні дані, визначені відповідними налаштуваннями доступу.

Результат бізнес-процесу: Користувач публічного порталу успішно отримав необхідну публічну інформацію про об'єкти нерухомого майна,

придатні або використовувані для проживання ВПО, згідно зі своїм запитом.

5.15.5.8. Робота з заявами про надання ОНМ для проживання ВПО

5.15.5.8.1. br-23. Подання заяв про надання ОНМ для проживання ВПО

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою забезпечення можливості для ВПО або уповноваженої ними особи подати засобами системи заяви про надання для проживання ОНМ, відомості про які містяться в системі.

Схема процесу

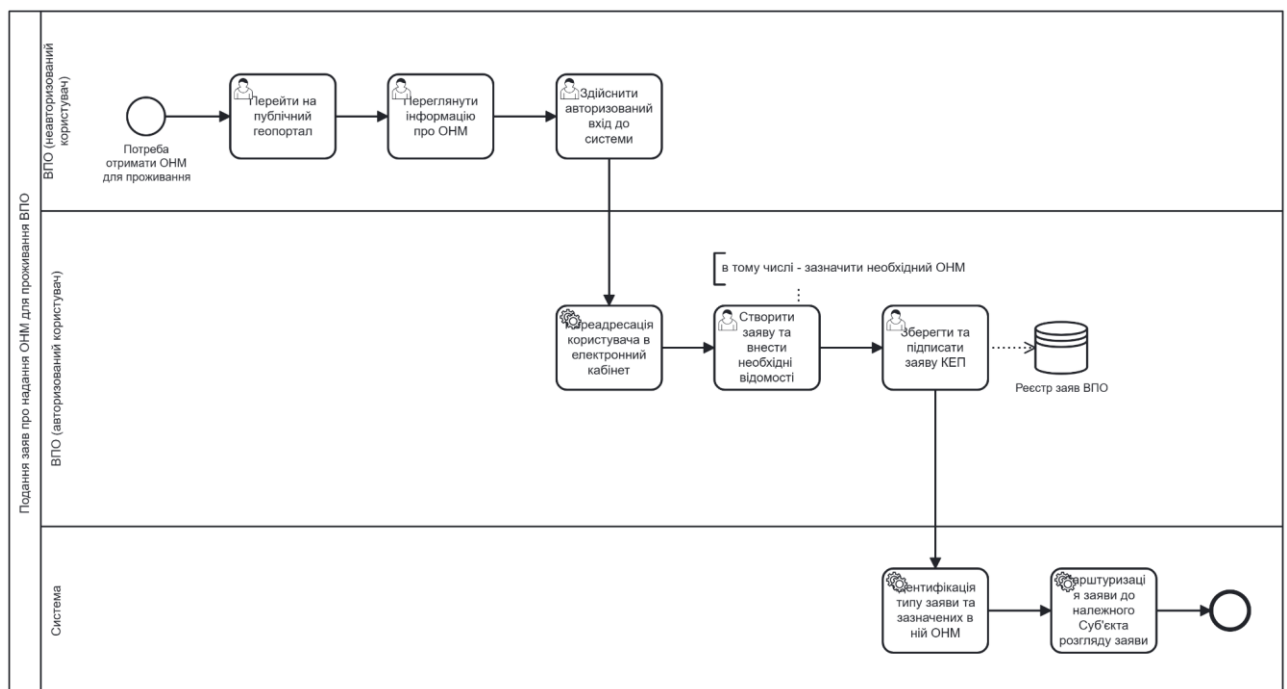


Схема бізнес-процесу. Подання заяв про надання ОНМ для проживання ВПО

camunda

<https://modeler.camunda.io/share/759556af-beb1-44e1-b6ab-a6449d819564>

Передумови:

- Користувач має доступ до інтернету та пристрій для роботи із системою.

- Користувач авторизований у системі та має призначену роль “ВПО” або є його уповноваженою особою.
- Користувач авторизований у системі та має призначену роль “власник ОНМ”, “орендар ОНМ” або є його уповноваженою особою.

Опис процесу:

- а. Неавторизований користувач (ВПО) переглядає інформацію про ОНМ на публічному порталі. Фільтрує дані відповідно до власних потреб. Отримує певну інформацію про ОНМ які відповідають критеріям його запиту.
- б. У разі спроби створення заяви Система пропонує користувачу здійснити вхід і пройти процедури автентифікації та авторизації.
- в. Неавторизований користувач (ВПО) здійснює вхід до системи та проходить автентифікацію та авторизацію.
- г. Після успішного входу Користувач автоматично перенаправляється до інтерфейсу створення заяви із збереженим вибором ОНМ, де він додає відповідну заяву про надання ОНМ для проживання, вносить інші відомості, визначені формою такого документу, зберігає та підписує ЕП.
- д. Система ідентифікує зазначені в ній ОНМ та здійснює маршрутизацію до належного електронного кабінету відповідного суб'єкта розгляду такої заяви.

Бізнес-правила:

1. Неавторизовані користувачі можуть переглядати відомості про ОНМ, але не можуть створювати заяви.
2. Заява автоматично маршрутизується відповідно до належного електронного кабінету відповідного суб'єкта розгляду такої заяви.
3. В рамках цього бізнес процесу ВПО не можуть подавати заявки щодо ОНМ які є земельними ділянками.

Результат бізнес-процесу: Користувач успішно подав заяву про надання ВПО для проживання ОНМ через свій електронний кабінет.

5.15.5.8.2. бр-24. Робота з заявами ВПО

Основні відомості. Даний бізнес-процес описує послідовність кроків, спрямованих на маршрутизацію та розгляд заяв ВПО щодо надання ОНМ для проживання.

Суб'єктом розгляду заяви виступають юридичні або приватні особи, які мають право приймати рішення щодо надання ОНМ для проживання ВПО. До таких суб'єктів належать:

- орендарі будівель, споруд і приміщень (їх окремих частин) закладів та установ освіти державної і комунальної форми власності;
- власники об'єктів нерухомого майна або уповноважені ними особи;
- уповноважені представники територіальної громади (органів місцевого самоврядування, утворених громадою);
- суб'єкти управління об'єктами державної власності.

У випадку, якщо суб'єкт розгляду не зареєстрований у Системі та/або не підтвердив свої повноваження щодо конкретного ОНМ, зазначеного в заяві, така заява автоматично не приймається до розгляду з надсиланням заявнику засобами Системи повідомлення щодо необхідності подання такої заяви поза Системою.

Схема процесу

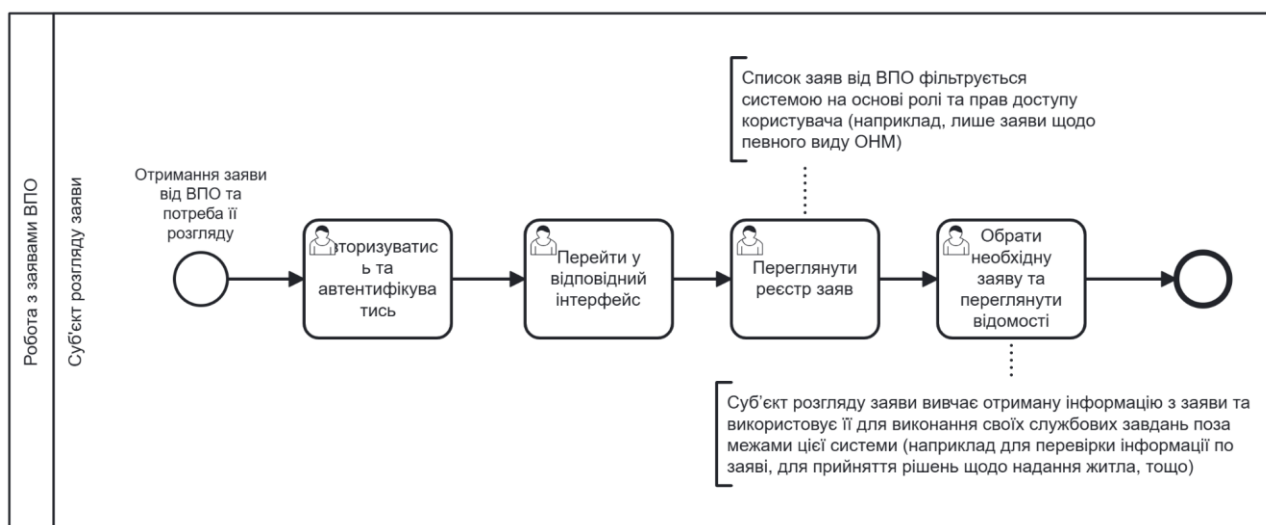


Схема бізнес-процесу. Робота з заявами ВПО

Передумови:

- Заява ВПО внесена в систему.
- Суб'єкт розгляду заяви автентифікований і авторизований у системі з роллю, що надає доступ до реєстру заяв.

Опис процесу:

- Суб'єкт розгляду заяви автентифікується та авторизується в системі як користувач з відповідною роллю.
- Система автоматично формує сповіщення Суб'єкту розгляду про надходження нових заяв від ВПО, що відповідають його ролі та територіальним повноваженням.
- Суб'єкт розгляду заяви здійснює навігацію в інтерфейсі електронного кабінету до розділу або функції, що дозволяє переглядати реєстр заяв.
- Система завантажує та відображає суб'єкту розгляду заяви список заяв від ВПО, який фільтруватися системою на основі ролі та прав доступу користувача (наприклад, лише заяви щодо певного виду ОНМ).
- Суб'єкт розгляду заяви обирає конкретну заяву зі списку, щоб переглянути її детальний зміст.
- Система завантажує та відображає деталі обраної заяви. Обсяг детальної інформації, доступної для перегляду, також обмежується правами доступу користувача.
- Суб'єкт розгляду заяви вивчає отриману інформацію з заяви та використовує її для прийняття відповідного рішення, зокрема, але не виключно, в рамках виконання своїх службових завдань поза межами цієї системи (наприклад для уточнення інформації по заяві, для прийняття рішень щодо надання житла, тощо).

Бізнес-правила:

- Суб'єкт розгляду заяви має доступ лише до тих заяв, що пов'язані з його повноваженнями та відповідними ОНМ.

Результат бізнес-процесу: Заява ВПО про надання їм для проживання ОНМ, відомості про які містяться в системі успішно переглянута відповідним суб'єктом розгляду заяви.

5.15.5.9. Робота зі статусами ОНМ

5.15.5.9.1. br-25. Робота зі статусами ОНМ

Основні відомості. Даний бізнес процес є послідовністю логічно пов'язаних кроків або дій, що виконуються з метою внесення в систему відомостей щодо статусу ОНМ в частині його використання ВПО. У межах даного бізнес-процесу під Власником ОНМ розуміються такі категорії суб'єктів:

- орендарі будівель, споруд і приміщень (у тому числі їх окремих частин), що належать закладам та установам освіти державної і комунальної форми власності;
- власники об'єктів нерухомого майна або уповноважені ними особи;
- уповноважені представники територіальних громад, зокрема органів місцевого самоврядування, утворених відповідними громадами;
- суб'єкти управління об'єктами державної власності.

Схема процесу

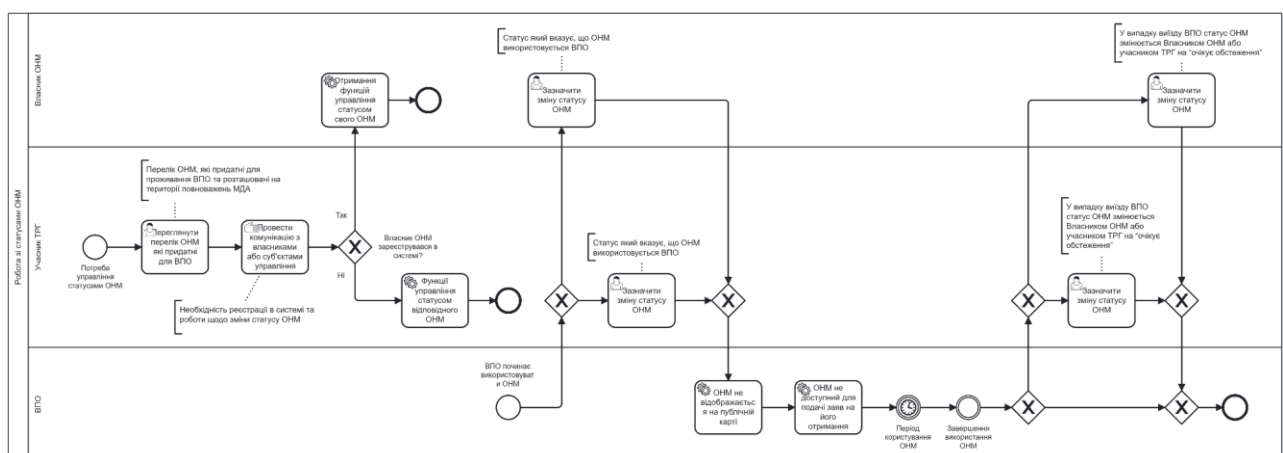


Схема бізнес-процесу. Робота зі статусами ОНМ

Передумови:

- Власник ОНМ зареєстрований та автентифікований у системі з роллю, яка надає доступ до управління статусами відповідними ОНМ.
- У випадку, якщо Власник ОНМ не зареєстрований у системі, функції роботи зі статусами ОНМ виконує учасник ТРГ, який входить до складу відповідної комісії з обстеження.

Опис процесу:

- а. Учасник ТРГ входить у систему та переглядає перелік ОНМ, які придатні для проживання ВПО та розташовані на території повноважень відповідної МДА.
- б. Учасник ТРГ здійснює (поза системою) координацію роботи з відповідним Власником ОНМ, для забезпечення його реєстрації та подальшої роботи із Системою.
- в. Власник ОНМ реєструється в системі або на етапі надання відомостей до координаційної комісії, або на подальших етапах, отримуючи доступ до функціоналу управління статусом своїх ОНМ, де він вносить зміни до статусу відповідного ОНМ ("вільно"/"використовується").
- г. Альтернативний крок (відсутність реєстрації власника (або суб'єкта управління): Якщо Власник ОНМ не реєструється в системі, функції з управління статусами ОНМ (зміна "вільно"/"використовується") виконує учасник ТРГ.
- д. У випадку підтвердження факту використання ВПО певного ОНМ (напр., на підставі договору або рішення) статус ОНМ змінюється змінюється Власником ОНМ або відповідним членом комісії (або учасником ТРГ).
- е. У випадку припинення ВПО використання відповідного ОНМ, статус ОНМ змінюється Власником ОНМ або відповідним членом комісії (або учасником ТРГ) на "очікує обстеження".

Примітка. Після виїзду ВПО, комісія з обстеження перевіряє стан ОНМ. Якщо комісія схвалює придатність ОНМ для подальшого проживання, ОНМ знову з'являється на публічній карті доступних об'єктів.

Бізнес-правила:

1. Змінювати статуси ОНМ можуть тільки користувачі з відповідними ролями.

У системі передбачено три верхньорівневі групи статусів (категорії) які можуть бути розширені користувачем з відповідною роллю

Таблиця. Верхньорівневі групи статусів

№	Категорія статусів	Приклади підвидів	Призначення
1	Придатність для проживання ВПО	придатний, непридатний, тимчасово непридатний	Визначає, чи може об'єкт бути використаний для тимчасового розміщення ВПО.
2	Статус заселення	заселений, заява на розгляді, вільний	Вказує фактичний стан використання об'єкта.
3	Технічний стан / готовність	потребує обстеження потребує будівництва, потребує реконструкції, потребує ремонту, потребує переоснащення	Використовується для об'єктів, що потребують певного виду робіт для відновлення або облаштування.

Кожен об'єкт ОНМ може мати комбінацію статусів із різних категорій, але лише по одному статусу в межах однієї категорії.

Результат бізнес-процесу: Статус ОНМ змінено відповідно факту використання або припинення використання цих об'єктів ВПО. Це забезпечує актуальність інформації про доступне житло та дозволяє ефективно управляти ресурсами для розміщення ВПО.

5.15.5.10. Робота з програмно-апаратними та/або методологічними помилками

5.15.5.10.1. бр-26. Подання повідомлення про виявлену програмно-апаратну та/або методологічну помилку

Основні відомості. Даний бізнес-процес описує послідовність дій користувача системи або користувача Електронного кабінету для повідомлення про виявлені під час роботи системи програмно-апаратні або методологічні помилки. Метою процесу є забезпечення своєчасної реєстрації та направлення повідомлення про помилку до відповідальних осіб (держателя та/або технічного адміністратора) для подальшого аналізу та усунення.

Схема процесу

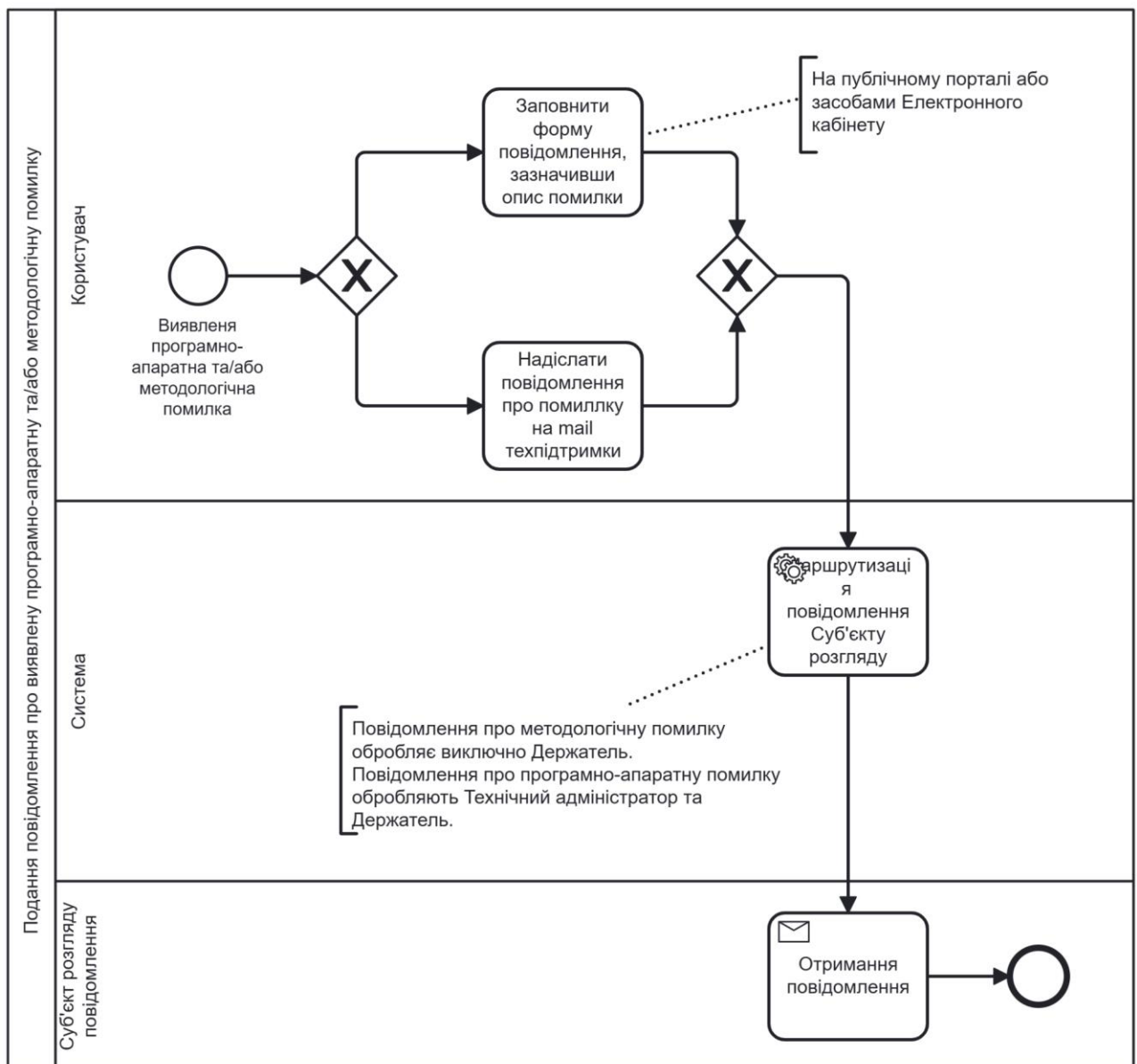


Схема бізнес-процесу. Подання повідомлення про виявлену програмно-апаратну та/або методологічну помилку

camunda

<https://modeler.camunda.io/share/78d3b8ed-8d26-429d-9831-f2boac579d6f>

Передумови:

- Під час роботи в системі користувач виявив некоректну роботу, розбіжність у даних, неправильну логіку функціонування або збій, що класифікується як помилка.
- Користувач має доступ до одного з каналів зв'язку: електронний кабінет, портал системи або електронна пошта.

Опис процесу:

- a. Користувач під час роботи з системою стикається з проблемою (наприклад, неможливість зберегти дані, некоректне відображення інформації, помилкові розрахунки, збій у роботі функції).
- b. Користувач засобами системи, через один з доступних інтерфейсів (електронний кабінет, портал) активує опцію подання повідомлення про помилку.
- c. Користувач намагається попередньо визначити тип помилки:
 - Методологічна помилка (пов'язана з невідповідністю бізнес-логіки системи нормативним актам, методикам розрахунків, встановленим процедурам);
 - Програмно-апаратна помилка (пов'язана з неправильною роботою програмного коду, інфраструктури, бази даних (напр., "зависання" сторінки, помилка 500, непрацюючі кнопки).
- d. Користувач заповнює форму повідомлення, зазначає з випадаючого списку тип помилка та відправляє його.
- e. Система автоматично переадресовує повідомлення належній стороні розгляду, в залежності від типу повідомлення.
- f. Як альтернативний варіант, Користувач може направити відповідне повідомлення на e-mail технічної підтримки, зазначений на порталі у відповідному розділі.

Бізнес-правила:

1. Будь-який користувач системи або Електронного кабінету має право надіслати повідомлення про виявлену помилку.
2. Повідомлення про методологічну помилку надсилається виключно держателю.
3. Повідомлення про програмно-апаратну помилку обов'язково надсилається одночасно і технічному адміністратору, і держателю.
4. Спосіб надання відповіді користувачу щодо його звернення залежить від того, яким каналом було отримано повідомлення про помилку.

Результат бізнес-процесу. Повідомлення про виявлену помилку успішно подано користувачем та доставлено держателю та/або технічному адміністратору.

5.15.5.10.2. br-27. Робота з повідомленнями про виявлену програмно-апаратну та/або методологічну помилку

Основні відомості. Даний бізнес-процес описує послідовність дій відповідальних осіб (держателя та технічного адміністратора) щодо розгляду повідомлень користувачів про виявлені під час роботи системи або Електронного кабінету програмно-апаратні та методологічні помилки.

Схема процесу

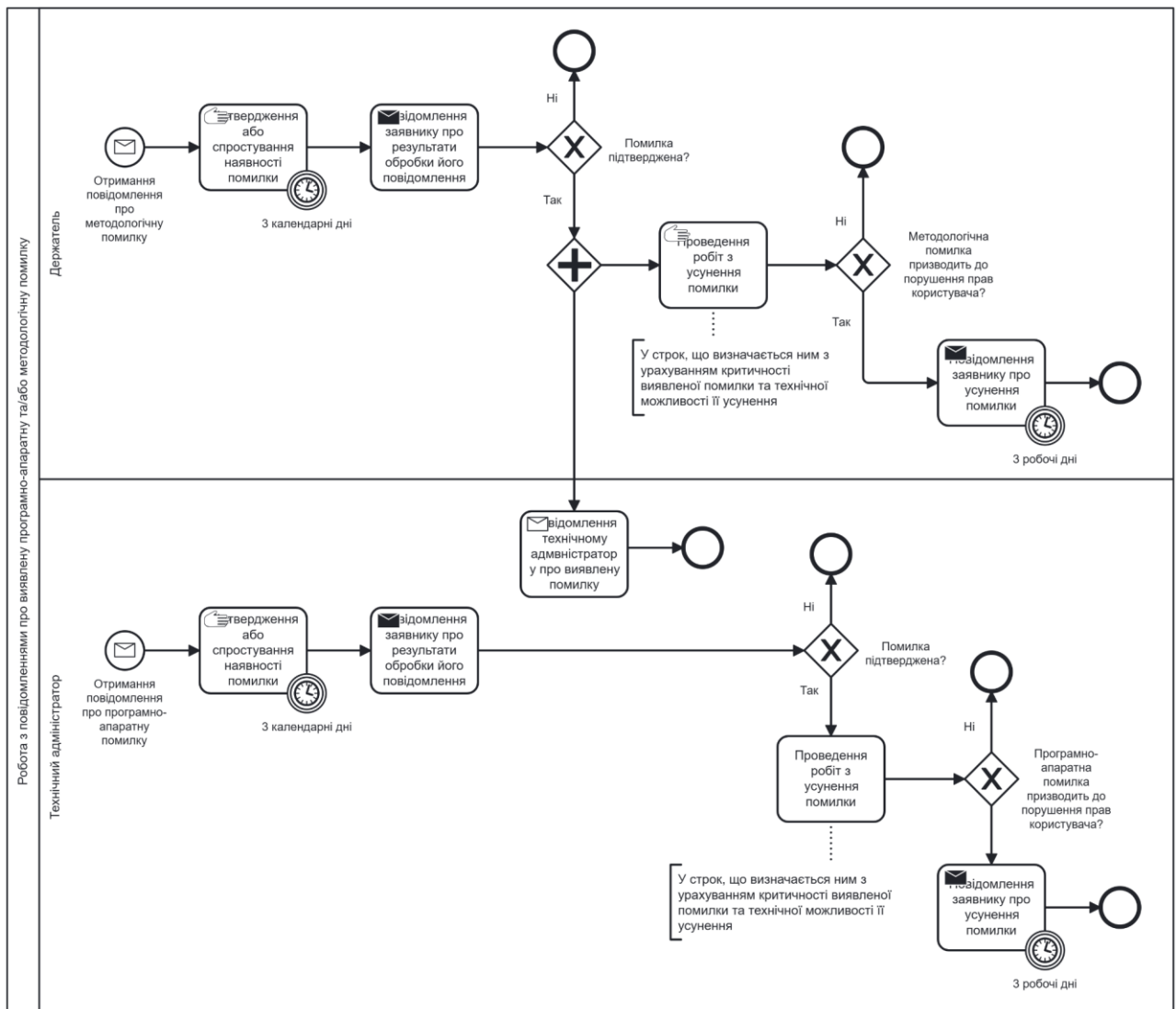


Схема бізнес-процесу. Робота з повідомленнями про виявлену програмно-апаратну та/або методологічну помилку

Передумови:

- Повідомлення про помилку успішно надійшло від користувача через електронний кабінет, портал або електронну пошту.
- Виявлена помилка класифікована як методологічна або програмно-апаратна.

Опис процесу:

- Після отримання повідомлення відповідний суб'єкт розгляду протягом 3 календарних днів перевіряє наявність методологічної або програмно-апаратної помилки та підтверджує або спростовує її факт. Користувач системи або електронного кабінету отримує повідомлення про результати обробки помилки через електронний кабінет та/або електронну пошту.
- У разі виявлення методологічної помилки держатель протягом трьох робочих днів повідомляє технічного адміністратора через Електронний кабінет для залучення його до усунення помилки.
- Якщо методологічна помилка або програмно-апаратна помилка призводить до порушення прав користувача системи або користувача Електронного кабінету, Держатель повідомляє такого Користувача через електронний кабінет або на адресу електронної пошти про помилку і про час, необхідний для її усунення та відновлення порушених прав такого користувача.
- Відповідний суб'єкт розгляду протягом трьох робочих днів інформує користувача про усунення помилки.

Бізнес-правила:

- Повідомлення про методологічну помилку обробляє виключно Держатель.
- Повідомлення про програмно-апаратну помилку обробляють Технічний адміністратор та Держатель.
- У разі недотримання Технічним адміністратором строку розгляду повідомлення (3 календарних дні), система автоматично формує повідомлення Держателю про порушення терміну первинної перевірки повідомлення.
- Підтвердження або спростування наявності помилки здійснюється протягом 3 календарних днів з моменту отримання повідомлення.

5. Термін усунення помилки визначається залежно від її критичності та технічної можливості.
6. Користувач інформується про результати перевірки та строки усунення помилки тим каналом, яким було отримано повідомлення.

Результат бізнес-процесу. Повідомлення про помилку розглянуто, наявність помилки підтверджено або спростовано, виконано усунення проблеми та відновлено працездатність системи. Користувач отримав інформацію про результати перевірки, строки усунення та відновлення порушених прав.

5.15.6. Опис моделі даних

5.15.6.1. Загальна структура

У складі інформаційної системи передбачено дві основні схеми даних:

- System schema – службові та довідкові дані: користувачі, ролі, права доступу, журнали подій, довідники (класифікатори, нормативні списки).
- Registry schema – бізнес-дані: реєстраційні записи (ОНМ, заяви, акти), документи та їхні версії з підписами (КЕП/ЕП), метадані реєстру.

Такий поділ забезпечує масштабованість, незалежність оновлень і підвищує безпеку.

5.15.6.2. Основні сутності

Сутності системи репрезентують логічно відокремлені об'єкти предметної області (наприклад, користувачі, об'єкти нерухомого майна, заяви, комісії), з визначеними атрибутами та взаємозв'язками.

5.15.6.2.1. Метамодель

Gist / Метадані сутності: описує атрибути й властивості сутностей (ID, назва, код, таблиця, статуси, інструкції, автори змін, версійність, можливість делегування прав).

5.15.6.2.2. Ідентифікація та доступ

User / Користувач: облікові записи, ідентифікаційні дані, контакти, статус.

Role / Роль: бізнес-ролі (CRUD-операції з протоколом комісії з обстеження, CRUD-операції з протоколом комісії з ОНМ, тощо, при чому можна вибрати або всі 4 системні права або, тільки деякі з них).

Permission / Дозвіл: атомарні права (операції), агрегуються у ролях.

RoleGroup / Група ролей: групування ролей для пакетного призначення.

Session / Сесія: дані автентифікації (MFA-метод, статус, час, IP).

Audit Log / Журнал аудиту: фіксація дій користувачів і системи.

Notification / Сповіщення: повідомлення користувачам (email, SMS, push).

API Key / API-ключ, OAuth Client / OAuth-клієнт: інструменти інтеграції зі сторонніми сервісами.

5.15.6.2.3. Організації та повноваження

Organization / Організація: юрособи, органи влади, інші суб'єкти.

Organizations_employees / Співробітники організації: перелік працівників із ролями та правом підпису.

Organizations_head / Керівник організації: історія керівників.

Commission / Комісія: постійні або тимчасові колективні органи.

User_commission / Члени комісії, User_trg / Члени ТРГ: склад колективних органів.

TRG / Тимчасова робоча група: створюється комісіями.

Rights_org / Повноваження організації, Rights_org_set / Налаштування, Rights_type / Типи повноважень: управління правами на території (області, райони).

DisplacedPerson / ВПО: дані про внутрішньо переміщених осіб (РНОКПП, ПІБ, адреса, номер довідки, унікальний ідентифікатор довідки, статус перевірки).

User_profile / Профіль користувача: розширені атрибути (посада, організація, уповноважена особа, ознаки власника ОНМ чи ВПО).

5.15.6.2.4. Об'єкти нерухомості

ONM Object / Об'єкт НМ: нерухомість (тип, площа, стан, статус, координати, власник, уповноважена особа).

Owner / Власник: юридичні та фізичні особи.

Address / Адреса: нормалізовані адресні дані (область, населений пункт, вулиця, координати) за стандартом КАТОТТГ.

Land_parcel / Земельна ділянка: кадастрові ділянки, прив'язані до ОНМ.

Application / Заява: подані заяви на ОНМ.

Inspection Act / Акт обстеження: результати огляду ОНМ комісією.

Media / Медіа: файли, що ілюструють ОНМ (фото, схеми, скани).

5.15.6.2.5. Документи та підпис

Document / Документ: офіційні документи, пов'язані із заявами й актами.

Document_version / Версія документа: історія редакцій.

External_doc / Зовнішні документи: скани чи посилання.

Reason / Причини змін: обґрунтування редакцій.

Signature / Підпис: дані про підписання (тип, дата, файл).

Signature_party / Підписант: користувачі, що підписали документ.

Data_storage / Сховище даних: збережені файли й хеші.

5.15.6.2.6. Інші сутності

Integration_sync / Синхронізація: відображення синхронізації з реєстрами.

Check / Перевірка: правила контролю правильності даних і документів.

Instructions / Інструкції: довідкові матеріали, прив'язані до сутностей.

5.15.6.3. Ключові зв'язки між сутностями

5.15.6.3.1. Ідентифікація та доступ

User —< user_role >— Role —< role_permission >— Permission (m-n).

User —< session >— Session (1-n).

Audit_log n-1 User, Audit_log n-1 Session.

User —< api_key >— API Key (1-n).

User —< oauth_client >— OAuth Client (1-n).

User —< user_delegation >— User (делегування доступу, m-n).

5.15.6.3.2. Організації та повноваження

Organization —< organizations_employees >— User (m-n).

Organization —< organizations_head >— User (1-n, історія).

Organization 1-n Commission.

Commission —< user_commission >— User (m-n).

Commission 1-n TRG.

TRG —< user_trg >— User (m-n).

Organization —< rights_org >— (rights_type, atu_unit) (m-n).

5.15.6.3.3. ВПО та користувачі

DisplacedPerson 1-n Application.

User 1-n Application (як заявник).

User_profile 1-1 User.

5.15.6.3.4. Об'єкти нерухомості

ONM —< onm_owner >— Owner (m-n, історія).

ONM —< onm_parcel >— Land_parcel (m-n).

ONM 1-n Address.

ONM 1-n Media.

ONM 1-n Application.

ONM 1-n Inspection_act.

Inspection_act n-1 Commission.

5.15.6.3.5. Документи та підпис

Application 1-n Document.

Inspection_act 1-n Document.

Document 1-n Document_version.

Document_version 1-1 Data_storage.

Document 1-n Signature.

Signature 1-n Signature_party (User).

Document 0..n External_doc.

Reason 1-n Document_version.

5.15.6.3.6. Інтеграції та контроль

Integration_sync (local_entity, local_id) ↔ source_system, external_id.

Notification n-1 User.

Check 1-n Document_type та Check 1-n Document.

Instructions 1-n Entity.

5.15.6.4. Технічні вимоги

Підтримка CRUD-операцій для всіх сутностей.

Аудит та логування всіх дій (користувач, IP, час, сутність, дія).

Контроль цілісності даних через PK, FK, UNIQUE, CHECK.

Історичність зв'язків (valid_from, valid_to) для власників ОНМ, ролей, повноважень, керівників.

Шифрування, перевірка та валідація КЕП/ЕП для всіх підписаних документів.

Масштабованість: розділення системних і реєстрових схем, оптимізація запитів.

Уніфікована модель інтеграції з зовнішніми реєстрами (Integration_sync).

Нормалізація довідкових даних (dict_document_type, dict_onm_type, dict_application_status тощо).

5.15.7. Розширений перелік атрибутів сутностей

Таблиця. User (Користувач)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ користувача
email	text	так	Електронна адреса для автентифікації та сповіщень
phone	text	ні	Номер телефону користувача
full_name	text	так	Повне ім'я користувача
status	text	так	Статус облікового запису: active blocked pending

Таблиця. Role (Роль)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ ролі
name	text	так	Системна назва ролі (унікальна)
description	text	ні	Опис призначення ролі

Таблиця. Permission (Дозвіл)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ дозволу
code	text	так	Системний код дозволу (унікальний)
description	text	ні	Опис дії/доступу

Таблиця. Organization (Організація)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ організації
reg_number	text	ні	Реєстраційний номер
edrpou	text	так	Код ЄДРПОУ
name	text	так	Назва організації
legal_status	text	ні	Правовий статус
phone	text	ні	Телефон організації
email	text	ні	Електронна пошта
site	text	ні	Веб-сайт організації
address	text	ні	Юридична/фактична адреса

Таблиця. OrganizationEmployee (Співробітник організації)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
org_id	uuid	так	Організація
full_name	text	так	ПІБ співробітника
rnokpp	text	так	РНОКПП

position	text	ні	Посада
right_sign	boolean	ні	Право підпису
dct_type	text[]	ні	Тип документів для підпису

Таблиця. OrganizationHead (Керівник організації)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
org_id	uuid	так	Організація
full_name	text	так	ПІБ керівника
rnokpp	text	так	РНОКПП
date_appointment	date	так	Дата призначення

Таблиця. Commission (Комісія)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ комісії
org_id	uuid	так	Організація
name	text	так	Назва комісії
type	text	так	Тип комісії
status	text	так	Статус чинності
date_created	date	так	Дата створення
date_closed	date	ні	Дата ліквідації

Таблиця. TRG (Тимчасова робоча група)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ TRG
commission_id	uuid	так	Комісія
org_id	uuid	так	Організація
status	text	так	Статус чинності
date_created	date	так	Дата створення
date_closed	date	ні	Дата ліквідації

Таблиця. DisplacedPerson (ВПО)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ запису ВПО
rnokpp	text	так	РНОКПП особи
full_name	text	так	ПІБ особи
certificate_number	text	так	Номер довідки ВПО
registry_uid	text	так	Унікальний ідентифікатор довідки в реєстрі ВПО
address	text	ні	Адреса за ЄДРА
status	text	ні	Статус перевірки

Таблиця. ONM_Object (Об'єкт нерухомого майна)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ об'єкта нерухомості
type	text	так	Тип об'єкта
owner_id	uuid	так	Власник об'єкта
address_id	uuid	так	Адреса об'єкта
capacity	integer	ні	Місткість
status	text	так	Статус доступності
geometry	geometry	ні	Геометрія

Таблиця. Application (Заява)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ заяви
onm_id	uuid	так	Об'єкт, на який подано заяву
user_id	uuid	так	Заявник
kind	text	так	Тип заяви
status	text	так	Статус
payload	jsonb	ні	Додаткові дані

Таблиця. InspectionAct (Акт обстеження)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ акта
onm_id	uuid	так	Об'єкт
commission_id	uuid	так	Комісія
date	date	так	Дата обстеження
result	text	ні	Результат

Таблиця. Document (Документ)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
type	text	так	Тип документа
version	integer	так	Номер версії
signed_by	uuid	ні	Хто підписав
signature	text	ні	Електронний підпис

Таблиця. ExternalDoc (Зовнішній документ)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
name	text	так	Назва документа
type	integer	так	Тип документа
path	text	ні	Шлях до документа
url	text	ні	Посилання

Таблиця. Reason (Підстава)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
reason_type	integer	так	Тип підстави
reason_body	text	ні	Опис підстави

Таблиця. Signature (Підпис)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
document_id	uuid	так	Документ
user_id	uuid	так	Користувач

date	date	так	Дата підпису
file	text	так	Файл підпису

Таблиця. DataStorage (Сховище)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
document_id	uuid	так	Документ
object_id	uuid	так	Об'єкт сутності
file	text	так	Файл
hash	text	так	Хеш файлу

Таблиця. Check (Перевірка)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
doc_type	text	так	Тип документа
name	text	так	Назва перевірки
query	text	так	Запит перевірки
check_type	integer	так	Тип перевірки: блокуюча/інформуюча

Таблиця. Instruction (Інструкція)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
entity_id	uuid	так	Сутність
text	text	так	Текст інструкції

Таблиця. IntegrationSync (Синхронізація інтеграцій)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
source_system	text	так	Зовнішня система/реєстр
local_entity	text	так	Локальна сутність
local_id	uuid	так	Ідентифікатор локальної сутності
external_id	text	ні	Зовнішній ідентифікатор

status	text	так	Статус синхронізації
--------	------	-----	----------------------

Таблиця. Notification (Сповіщення)

Назва	Тип	Обов'язковість	Опис
id	uuid	так	Первинний ключ
user_id	uuid	ні	Отримувач
channel	text	так	Канал: email sms system
subject	text	ні	Тема
body	text	ні	Текст
status	text	так	Статус відправки

Рисунок. UML-діаграма класів. ВПО, заявки та ОНМ

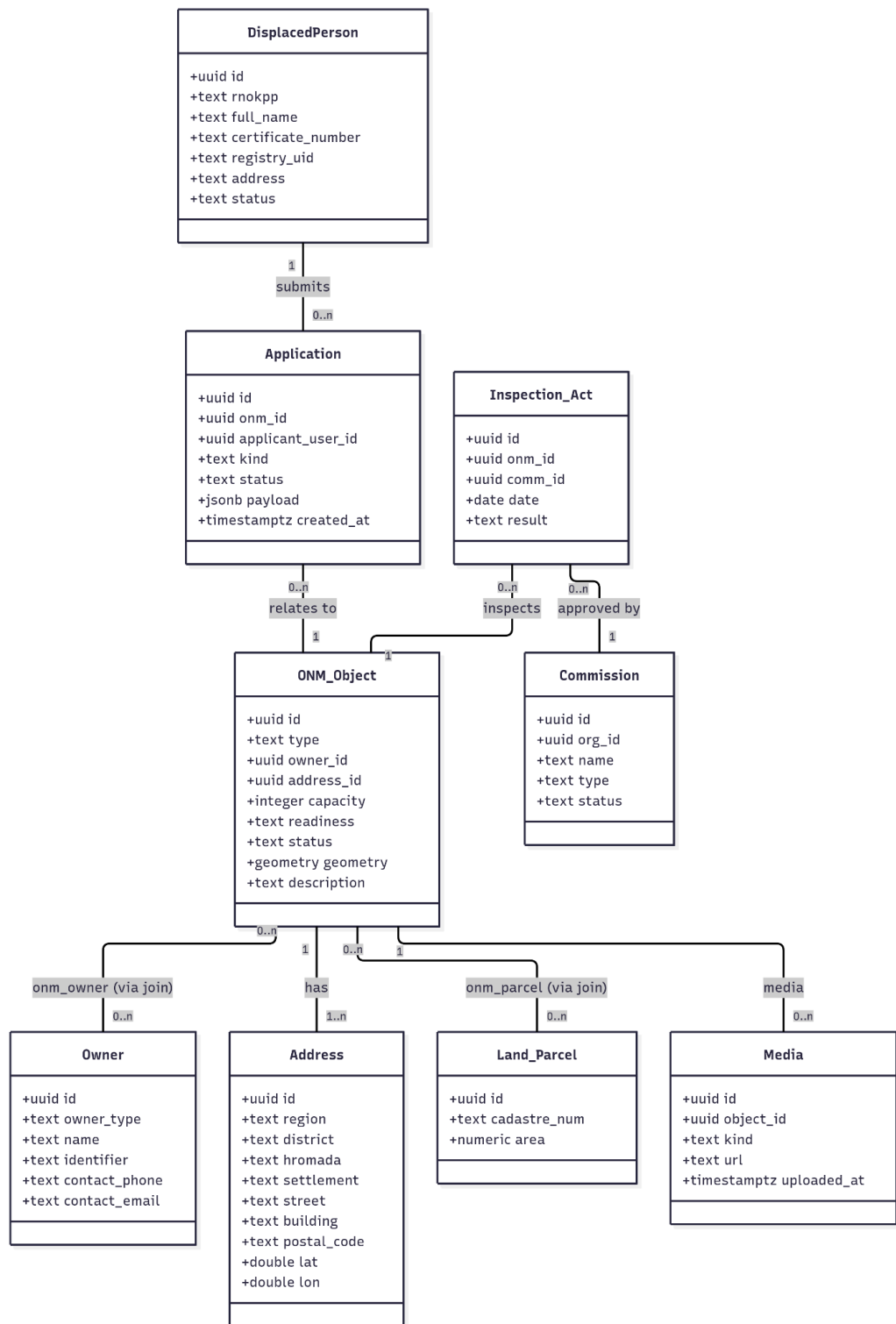


Рисунок. UML-діаграма класів. Документи, підписи, версії, сховище

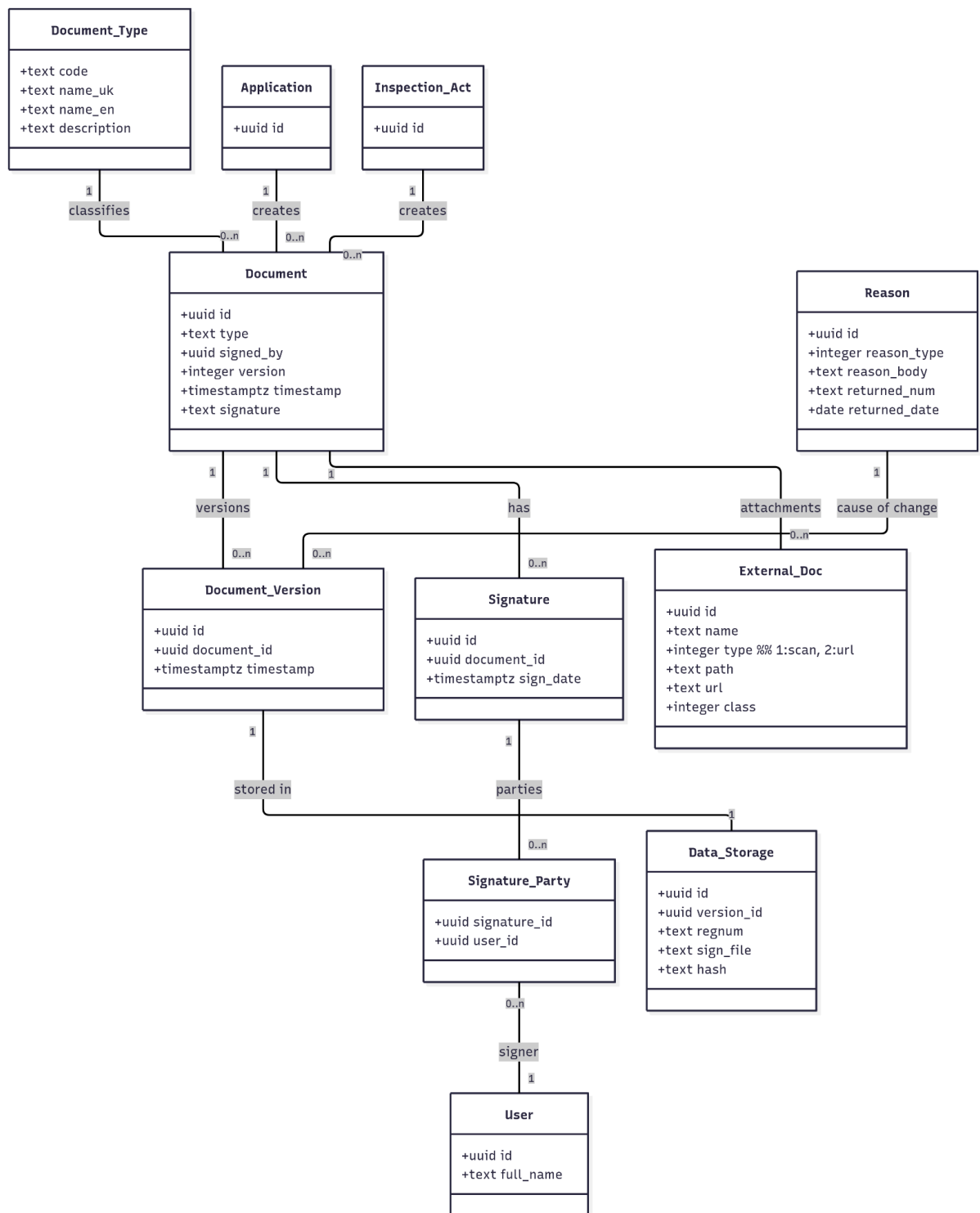


Рисунок. UML-діаграма класів. Інтеграції, сповіщення, аудит, перевірки, інструкції

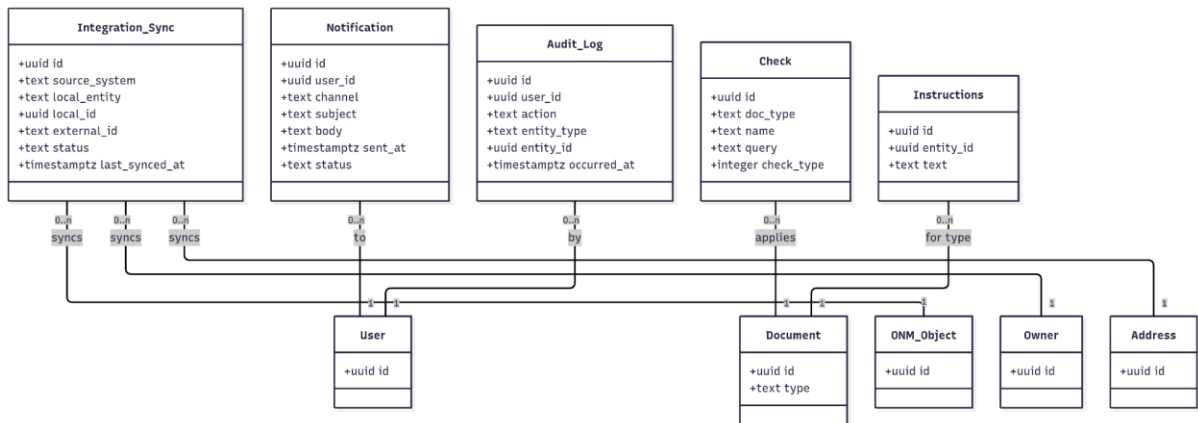
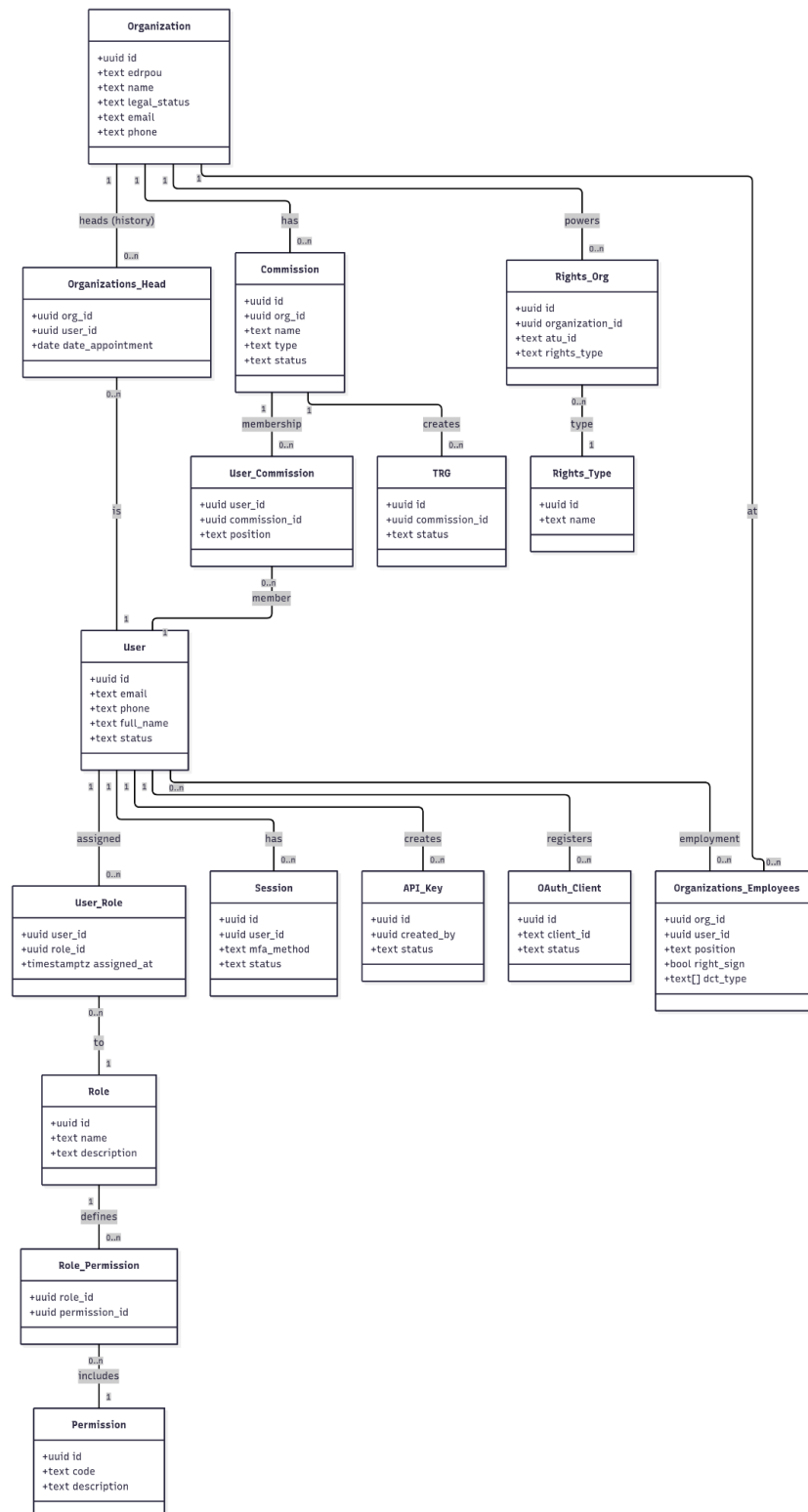


Рисунок. UML-діаграма класів. Користувачі і організації



5.15.8. Документи в системі

В цьому розділі визначено перелік основних документів, що використовуються в Системі для забезпечення реалізації функціональних можливостей системи та підтримки бізнес-процесів.

Документи є цифровими відображеннями формалізованих даних або завантажених файлів, що супроводжують бізнес-процеси (наприклад, заяви, рішення комісій, акти огляду).

Система повинна забезпечувати централізоване зберігання, контроль редакцій, можливість пошуку, фільтрації та перегляду документів відповідно до прав доступу та ролей користувачів.

В системі повинна забезпечуватись роботи з сутностями, наведеними в таблиці нижче.

До системи користувачами електронних кабінетів завантажуються (або створюються з її використанням) документи, зазначені в таблиці нижче.

Таблиця. Базові документи, що завантажуються або створюються в системі

№	Скорочена назва	Повна назва
1	Протокол координаційної комісії	Протокол засідання координаційної комісії з обліку ОНМ для проживання ВПО при обласних, Київській міській держадміністрації (військових адміністраціях) та додатки до нього
2	Протокол комісії з обстеження ОНМ	Протокол комісії з обстеження ОНМ для проживання ВПО при районних, районних у м. Києві держадміністраціях (військових адміністраціях) та додатки до нього
3	Акт обстеження ОНМ	Акт обстеження об'єктів нерухомого майна
4	Заява ВПО про надання для проживання ОНМ	Заява внутрішньо-переміщеної особи про надання для проживання об'єктів нерухомого майна

5.15.9. Функціональні компоненти

5.15.9.1. МОДУЛЬ “АВТОРИЗАЦІЯ КОРИСТУВАЧІВ”

5.15.9.1.1. Опис та призначення

Модуль повинен забезпечувати можливість використання технічним адміністратором додаткових (багатофакторних) механізмів автентифікації користувачів електронного кабінету для окремих категорій користувачів та/або окремих операцій, зокрема під час підписання електронних документів.

Механізми багатофакторної автентифікації повинні включати можливість:

- електронної ідентифікації за допомогою інформаційно-комунікаційної системи мобільної ідентифікації;
- накладення кваліфікованого електронного підпису (КЕП);
- підтвердження дії за допомогою додаткового методу ідентифікації, зокрема одноразового пароля (ОТР), надісланого через визначений канал зв'язку (SMS, мобільний застосунок тощо).

Система також повинна дозволяти налаштовувати умови застосування багатофакторної автентифікації залежно від типу користувача, ролі в системі та виду операції.

Користувачі електронних кабінетів (крім посадових осіб державних органів, місцевих держадміністрацій (військових адміністрацій), органів місцевого самоврядування) отримують доступ до електронного кабінету після проходження процедури електронної ідентифікації та автентифікації через державну інтегровану систему електронної ідентифікації та авторизуються автоматично програмними засобами системи залежно від їх правового статусу.

5.15.9.1.2. Функціональні вимоги

У процесі розробки мають бути враховані такі функціональні вимоги до Модуля

- Система повинна забезпечувати авторизацію користувачів після успішної автентифікації та перевірки їхніх облікових даних.

- Система повинна реалізовувати авторизацію на основі ролей (role-based access control), призначаючи кожному користувачу одну або декілька ролей відповідно до його повноважень.
- Система повинна забезпечувати можливість призначення прав доступу до функцій і даних окремо для кожної ролі.
- Система повинна підтримувати контекстну авторизацію за територіальним принципом — користувач може мати доступ лише до даних, що належать його територіальній юрисдикції.
- Система повинна перевіряти відповідність наданих ролей користувачам встановленим правилам і політикам безпеки (неможливість призначення заборонених комбінацій ролей).
- Система повинна забезпечувати можливість зміни ролей і прав користувачів у разі зміни їхніх обов'язків або статусу.
- Система повинна автоматично обмежувати доступ користувачів у разі закінчення терміну дії їхніх повноважень або деактивації облікового запису.
- Система повинна вести журнал усіх подій, пов'язаних з авторизацією (успішна/неуспішна спроба доступу, призначення ролей, зміна прав, обмеження доступу).

5.15.9.2. МОДУЛЬ “ЕЛЕКТРОННИЙ КАБІНЕТ”

5.15.9.2.1. Опис та призначення

Електронний кабінет користувача є модулем системи, який забезпечує електронну взаємодію між фізичними та юридичними особами, державними органами, органами місцевого самоврядування, в рамках створення та функціонування Системи. Основними принципами функціонування кабінету є:

- автоматизація процесів створення, реєстрації, підписання та зберігання документів в середовищі Системи;
- наявності інтерфейсів електронного сервісу, який максимально повно забезпечує можливість реалізації повноважень та можливостей користувачі;
- спрощення процедур інформаційної взаємодії учасників бізнес-процесів процесів та прискорення електронного документообігу між ними;

- забезпечення використання державної мови у всіх користувацьких інтерфейсах;
- автоматична перевірка програмними засобами електронного кабінету повноти та відповідності даних у створених користувачами електронних документах;
- розподіл прав доступу на підставі повноважень користувачів електронного кабінету;
- автоматичний контроль наповненості та підтвердження цілісності реєстраційних даних та обов'язкових полів документів.

Доступ до електронного кабінету надається користувачам після проходження електронної ідентифікації за допомогою інтегрованої системи електронної ідентифікації та відповідно до вимог Закону України «Про електронні довірчі послуги», Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, затвердженого постановою Кабінету Міністрів України від 19 вересня 2018 року № 749.

5.15.9.2.2. Опис функцій основних складових електронного кабінету

Таблиця. Опис функцій основних складових електронного кабінету

Назва складової	Опис функцій
Реєстр об'єктів	<p>відображення колонок з інформацією в табличному реєстрі;</p> <p>посторінкове відображення даних в табличному реєстрі;</p> <p>експорт інформації про об'єкти реєстру у формат xlsx, csv;</p> <p>пошук об'єктів за текстовим запитом;</p> <p>відбір об'єктів (фільтрація) з наступними можливостями;</p>

	редагування даних табличного реєстру при натисненні на відповідну комірку редагування в таблиці;
Картка об'єкта	<p>відображення всього ряду інформації, яка зберігається про об'єкт в базі даних системи;</p> <p>відображення просторового положення об'єкта на карті;</p> <p>відображення прикріплених фото (галереї фотографій);</p> <p>можливість прикріплення документів, максимальна кількість яких може встановлюватись адміністратором;</p> <p>відображення інформації по зміні об'єкта (ким і коли було створено об'єкт, хто і коли востаннє його відредагував);</p>
Форма внесення (редагування) відомостей (даних)	<p>внесення текстової інформації, інформації з довідників, числової інформації, геометрії об'єктів, зображення, файлів;</p> <p>інформація у формі має бути розділена на групи відповідним заголовком;</p> <p>випадаючі списки у формі повинні формуватися на основі довідників чи інших реєстрів в системі;</p> <p>поля для внесення чисел мають контролюватися на внесення невідповідних символів;</p> <p>випадаючі списки, які формуються на основі значної кількості інформації мають підвантажуватися лише за запитом користувача, а не в повному об'ємі (для зменшення апаратного навантаження на систему);</p>
Картографічне подання об'єктів реєстру	<p>відображення об'єктів на карті в якості точкових, лінійних чи полігональних об'єктів;</p> <p>відображення точкових об'єктів піктограмами;</p> <p>відображення різними кольорами об'єктів реєстру відповідно до статусу;</p>

	<p>відбір об'єктів на карті за допомогою системи фільтрів;</p> <p>вибір об'єкта на карті для отримання про нього інформації по кліку (об'єкти реєстру на карті мають бути інтерактивними).</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Система реалізує функціонал автоматичного інформування користувачів про наближення або настання визначених строків виконання дій з документами чи завданнями, що встановлюється бізнес-логікою процесів. При наближенні (або завершенні) встановленого терміну система формує та надсилає користувачу повідомлення-нагадування про необхідність виконання відповідних дій. Функція має виключно інформаційний характер і не обмежує подальшу роботу користувача або виконання процесів у системі.

5.15.9.2.3. Електронний кабінет уповноваженої особи МДА

Електронний кабінет забезпечує автоматизацію процесів внесення та ведення відомостей про координаційні комісії та комісії з обстеження, створені при відповідних місцевих державних адміністраціях (військових адміністраціях). Кабінет дозволяє керувати складом комісій, призначати ролі їх учасникам та забезпечувати належний доступ до документів і функцій системи відповідно до ролей користувачів.

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- внесення в систему (або внесення змін) персонального складу координаційної комісії або комісії з обстеження відповідної адміністрації;
- внесення контактних даних, ідентифікаторів членів комісії (напр. РНОКПП, паспорт) та інших відомостей;
- призначення ролей членам комісії (наприклад, «Голова комісії», «Секретар комісії», «Член комісії»);
- внесення відомостей акта про створення та затвердження положення комісії;
- підписання внесених відомостей за допомогою електронного підпису;

- перегляд відомостей про персональний склад комісії;
- підтримка процесу відкладеної авторизації для незареєстрованих членів комісії.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольових доступ до функцій кабінету

Роль	Функції
Уповноважена особа МДА	Додає та редагує відомості про членів комісії, призначає ролі, підписує внесені відомості електронним підписом, виконує CRUD-операції у межах системних прав ролі

5.15.9.2.4. Електронний кабінет координаційної комісії

Електронний кабінет забезпечує автоматизацію роботи координаційних комісій, створених при обласних, Київській міській державних адміністраціях (військових адміністраціях).

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- перегляд відомостей про персональний склад координаційної комісії;
- внесення відомостей про склад та зміни до складу ТРГ, перегляд відомостей про ТРГ координаційної комісії;
- додавання та перегляд відомостей протоколу засідання координаційної комісії;
- перегляд комісій з обстеження утворених в межах відповідної області, Київської міської державної адміністрації (військової адміністрації);
- перегляд актів обстеження, складених відповідними комісіями з обстеження;
- перегляд та внесення відомостей про ОНМ.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольових доступ до функцій кабінету

Роль	Функції
Голова координаційної комісії	Працює з інтерфейсами Електронного кабінету, виконує CRUD-операції у межах системних прав ролі та підписує документи у межах територіальних повноважень організації.
Секретар координаційної комісії	Працює з інтерфейсами Електронного кабінету, переглядає документи та завантажує файли. Виконує CRUD-операції у межах системних прав ролі та підписує документи визначені уповноваженою особою організації у межах територіальних повноважень організації. Управляє відомостями про ТРГ.
Член координаційної комісії	Працює з інтерфейсами Електронного кабінету, виконує CRUD-операції у межах системних прав ролі.

5.15.9.2.5. Електронний кабінет комісії з обстеження

Електронний кабінет забезпечує автоматизацію роботи комісій з обстеження, створених при районних державних адміністраціях (військових адміністраціях).

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- перегляд відомостей про відповідну координаційну комісію;
- перегляд відомостей про персональний склад комісії з обстеження;
- внесення відомостей про склад та зміни до складу ТРГ, перегляд відомостей про ТРГ комісії з обстеження;
- додавання та перегляд відомостей протоколу засідання комісії з обстеження;
- додавання відомостей Акту обстеження ОНМ з додатками та перегляд;
- перегляд та внесення інформації про ОНМ.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольовий доступ до функцій кабінету

Роль	Функції
Голова комісії з обстеження	Працює з інтерфейсами Електронного кабінету, виконує CRUD-операції у межах системних прав ролі та підписує документи у межах територіальних повноважень організації.
Секретар комісії з обстеження	Працює з інтерфейсами Електронного кабінету, виконує CRUD-операції у межах системних прав ролі та підписує документи визначені уповноваженою особою організації межах територіальних повноважень організації. Зокрема виконує CRUD-операції з відомостями про ТРГ.
Член комісії з обстеження	Працює з інтерфейсами Електронного кабінету, виконує CRUD-операції у межах системних прав ролі.

5.15.9.2.6. Електронний кабінет учасника Тимчасової робочої групи Координаційної комісії

Електронний кабінет забезпечує підтримку та автоматизацію роботи тимчасових робочих груп, створених координаційними комісіями при обласних, Київській міській та районних державних адміністраціях (військових адміністраціях).

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- перегляд відомостей про персональний склад координаційної комісії;
- перегляд відомостей протоколу засідання координаційної комісії;
- перегляд актів обстеження, складених відповідними комісіями з обстеження;

- перегляд та внесення інформації про ОНМ.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольовий доступ до функцій кабінету

Роль	Функції
Учасник ТРГ координаційної комісії	Працює з інтерфейсами Електронного кабінету, переглядає відомості про координаційну комісію, протоколи її засідань, акти обстеження та інформацію про ОНМ. Має можливість вносити відомості про ОНМ (онбординг) у передбаченому форматі.

5.15.9.2.7. Електронний кабінет учасника Тимчасової робочої групи комісії з обстеження

Електронний кабінет забезпечує підтримку та автоматизацію діяльності тимчасових робочих груп, створених комісіями з обстеження при районних державних адміністраціях (військових адміністраціях).

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- перегляд відомостей про персональний склад комісії з обстеження;
- перегляд відомостей протоколів засідання комісії з обстеження;
- перегляд актів обстеження, складених відповідними комісіями з обстеження;
- перегляд та внесення інформації про ОНМ.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольовий доступ до функцій кабінету

Роль	Функції
Учасник ТРГ комісії з	Працює з інтерфейсами Електронного

обстеження	кабінету, переглядає відомості про комісію з обстеження, протоколи її засідань, акти обстеження та інформацію про ОНМ. Має можливість роботи зі статусами ОНМ.
------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------

5.15.9.2.8. Електронний кабінет Держателя

Електронний кабінет забезпечує автоматизацію окремих функцій, пов'язаних з моніторингом даних для посадових осіб Мінрозвитку, що циркулюють в системі.

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- моніторинг стану функціонування системи, у тому числі отримання автоматичних повідомлень про виявлені збої або недоліки;
- інформування технічного адміністратора про виявлені проблеми та передача пропозицій щодо їх усунення через інтегрований механізм зворотного зв'язку;
- робота з повідомленнями про методологічні помилки та програмно-апаратну помилку;
- доступ до аналітичного дашборду, що відображає ключові показники роботи системи, стан інтеграцій, дані в системі та інші релевантні метрики для прийняття управлінських рішень.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольових доступ до функцій кабінету

Роль	Функції
Держатель	Має доступ до даних та сервісів ІАС у межах своїх повноважень, інформує технічного адміністратора про виявлені проблеми та подає пропозиції щодо удосконалення функціонування системи, має доступ до аналітичного дашборду з ключовими показниками роботи системи та станом

	інтеграцій.
--	-------------

5.15.9.2.9. Електронний кабінет Адміністратора

Електронний кабінет забезпечує автоматизацію функцій адміністрування та підтримки роботи системи.

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- адміністрування системи, включаючи управління користувачами, ролями, доступами, налаштування сервісів та довідників;
- управління доступом до електронних кабінетів, в частині надання, блокування, анулювання та відновлення доступу користувачам у випадках, передбачених нормативними актами;
- перегляд журналу всіх дій та/або подій, що відбуваються в системі;
- контроль за резервним копіюванням, безпекою даних та дотриманням політик захисту інформації.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольових доступ до функцій кабінету

Роль	Функції
Адміністратор	Працює з інтерфейсами адміністратора.

5.15.9.2.10. Електронний кабінет Технічного адміністратора

Електронний кабінет забезпечує автоматизацію функцій технічного адміністрування та підтримки роботи системи.

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- забезпечення обміну даними між ІАС та іншими електронними інформаційними ресурсами, налаштування інтеграцій;

- проведення технічних та технологічних заходів із надання, блокування та анулювання доступу до ІАС;
- робота з повідомленнями про методологічні помилки та програмно-апаратні помилки;
- перегляд журналу всіх дій та/або подій, що відбуваються в системі;
- підтримка в актуальному стані класифікаторів, довідників, словників та баз даних ІАС, автоматизоване або ручне оновлення інформації.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольових доступ до функцій кабінету

Роль	Функції
Технічний адміністратор	Працює з інтерфейсами технічного адміністратора, що забезпечують технічне адміністрування.

5.15.9.2.11. Електронний кабінет Власника ОНМ

Електронний кабінет забезпечує розгляд заяв внутрішньо переміщених осіб та уповноважених осіб через систему.

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- доступ даних про відповідні ОНМ;
- отримання та перегляд заяв, поданих ВПО або уповноваженими ними особами, щодо надання для тимчасового проживання ОНМ, що перебувають у власності або управлінні користувача;
- управління статусами ОНМ.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольових доступ до функцій кабінету

Роль	Функції
------	---------

Власник ОНМ/уповноважена особа	Має доступ до відомостей та документів щодо об'єктів нерухомого майна, що перебувають у їх власності або управлінні, переглядає заяви ВПО про надання житла для тимчасового проживання, вносить відомості щодо статусів відповідних ОНМ.
Суб'єкт управління державним/комуналь ним майном	

5.15.9.2.12. Електронний кабінет Орендаря

Електронний кабінет забезпечує автоматизацію доступу до даних про орендовані об'єкти нерухомого майна та розгляду заяв внутрішньо переміщених осіб через систему.

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- доступ даних про ОНМ, що перебувають в оренді користувача (орендаря або уповноваженої особи);
- отримання та перегляд заяв, поданих ВПО або уповноваженими ними особами, щодо надання для тимчасового проживання ОНМ, що перебувають в оренді користувача (орендаря або уповноваженої особи);
- управління статусами ОНМ.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольових доступ до функцій кабінету

Роль	Функції
Орендар/уповноваже на особа	Має доступ до відомостей та документів щодо орендованих об'єктів нерухомого майна, переглядає заяви ВПО про надання житла для тимчасового проживання, вносить відомості щодо статусів відповідних ОНМ..

5.15.9.2.13. Електронний кабінет ВПО

Електронний кабінет забезпечує автоматизацію доступу до інформації та подання заяв щодо отримання житла для внутрішньо переміщених осіб засобами системи.

В межах Електронного кабінету реалізуються наступні функціональні можливості, обсяг яких визначається відповідною роллю користувача:

- перегляд актуальної інформації про ОНМ, їх характеристики та умови надання для тимчасового проживання ВПО;
- можливість подавати електронні заявки власникам ОНМ, уповноваженим ними особам, представникам територіальних громад, суб'єктам управління об'єктами державної власності та орендарям будівель, споруд, приміщень закладів і установ освіти державної та комунальної форми власності, що надають житло для тимчасового проживання ВПО.

Електронний кабінет має використовувати рольову модель, що визначає різні рівні доступу до функцій та даних:

Таблиця. Рольових доступ до функцій кабінету

Роль	Функції
ВПО/уповноважена особа	Має доступ до актуальної інформації про об'єкти нерухомого майна, може подавати електронні заявки на отримання житла для тимчасового проживання та отримує повідомлення про їх розгляд.

5.15.9.3. МОДУЛЬ “ПОРТАЛ”

5.15.9.3.1. Загальні відомості

Модуль “Портал” є компонентом системи, що функціонує як комплекс програмно-технічних засобів, мережових та геоінформаційних сервісів, що призначені для:

- авторизованого доступу користувачів до електронного кабінету;

- надання користувачу інформації щодо функціонування системи;
- надання інформації про нормативно-правові акти, які регулюють питання функціонування системи;
- надання інформації про проведення профілактичних та/або технічних робіт з підтримки системи;
- можливість надати повідомлення про наявність програмно-апаратних та методичних помилок у роботі Системи;
- перегляду користувачем системи публічної інформації, що міститься в системі та підлягає оприлюдненню відповідно до Закону України “Про доступ до публічної інформації”, у тому числі в форматі відкритих даних, із забезпеченням відкритого доступу до відповідної інформації, зокрема у формі загальнодоступної інтерактивної карти.

5.15.9.3.2. Функціональні вимоги

Портал повинен забезпечувати час відповіді сервісу не більше 3 секунд для початкової реакції на запит користувача. Подальше завантаження великих обсягів геопросторових даних здійснюється асинхронно із застосуванням механізмів кешування, тайлінгу, генералізації та оптимізації відображення.

Для зображення розміром 470 кілобайт (наприклад, 800 × 600 пікселів із глибиною кольору 8 біт) час відповіді для надсилання початкової відповіді на запит на отримання карти до сервісу перегляду має становити максимум 5 секунд у звичайній ситуації. Нормальна ситуація – періоди поза піковим навантаженням. Він встановлений на 90% часу.

До дизайну Порталу висуваються вимоги, затверджені для офіційних веб-сайтів (веб-порталів) органів виконавчої влади та офіційних веб-ресурсів, що пов’язані з діяльністю органів виконавчої влади наказом Міністерства цифрової трансформації України від 23.06.2022 №57.

Сторінки не повинні бути перевантажені інформаційно-графічними матеріалами. Глибина вкладення (логічних переходів) не повинна бути більше 5 рівнів. Побудова логічних зв’язків в межах певної функціональності повинна бути зручною та інтуїтивно зрозумілою.

Всі інтерактивні елементи повинні бути виконані у зручному та зрозумілому вигляді, представленні із набором відповідних текстових та/або графічних інформаційних підказок.

Доступ до геопросторових даних та метаданих на геопорталі має забезпечуватись наступними геоінформаційними сервісами:

- веб-сервіс каталогу метаданих, CSW (Catalogue Services for the Web);
- веб-картографічний сервіс, WMS (Web Map Service);
- веб-сервіс картографічних тайлів, WMTS (Web Map Tile Service);
- веб-сервіс просторових об'єктів, WFS (Web Feature Service);
- веб-сервіс покриття, WCS (Web Coverage Service).

Портал повинен містити розділ з інструкціями для користувачів щодо використання основних функцій, а користувачі повинні мати доступ до контактів технічної підтримки.

Портал також повинен забезпечувати можливість подання повідомлень про виявлені програмно-апаратні та методологічні помилки до технічної підтримки через спеціальну електронну форму. Подані через форму звернення мають автоматично надходити до відповідних фахівців для подальшого опрацювання. Система повинна забезпечувати відстеження статусу розгляду звернення та інформування користувача про його результат.

Портал повинен забезпечувати технічну оптимізацію для пошукових систем (SEO), включаючи коректне формування мета-тегів (title, description, keywords, OpenGraph), оптимальну для індексації структуру URL, наявність файлів robots.txt та sitemap.xml. Для підвищення якості представлення даних у пошукових системах має застосовуватися семантична розмітка на основі стандартів schema.org із використанням JSON-LD.

Крім того, Портал повинен відповідати вимогам стандарту WCAG 2.1 (мінімум рівень AA), що передбачає доступність контенту для людей з обмеженими можливостями, зокрема сумісність з екранними читачами,

коректну навігацію за допомогою клавіатури, достатній контраст кольорів та масштабованість інтерфейсу.

5.15.9.4. МОДУЛЬ “ДОКУМЕНТИ ТА ФАЙЛИ”

5.15.9.4.1. Загальні відомості

Модуль «Документи та файли» призначений для стандартизації та автоматизації процесу роботи користувача з документами які створюються в рамках бізнес-процесів. В цілому модуль має забезпечувати реалізацію наступних механізмів:

- підтримка багаторівневої системи доступу до документів відповідно до ролей користувачів та відповідних бізнес-процесів;
ведення історії версій документів, що дозволяє відслідковувати всі внесені зміни, із збереженням доступу до попередніх редакцій;
- можливість накладання кількох електронних підписів різних користувачів згідно з відповідними бізнес-процесами;
- автоматичний контроль строків роботи з документами, що дозволяє Системі відслідковувати визначені терміни виконання дій з документами та автоматично надсилати повідомлення про їх завершення та необхідність вчинення дії відповідними користувачам;
- зберігання метаданих щодо кожного документа (напр. автор, дата створення, останньої зміни, статус документа, тощо);
- резервне копіювання та відновлення документів і файлів з дотриманням політик збереження даних.

Кожному електронному документу під час створення автоматично надається внутрішній ідентифікаційний номер, який є незмінним, у тому числі в разі внесення змін та доповнень до нього, виправлення технічних помилок.

У Системі має бути реалізована підтримка версійності документів із можливістю відстеження історії змін та доступом до попередніх редакцій, що зберігаються у вигляді окремих версій із відповідними мітками часу.

Створення електронних документів засобами Системи здійснюється користувачами електронного кабінету шляхом заповнення відповідних відомостей (даних) в ній.

Створення електронного документа в Системі завершується його підписанням електронним підписом користувача. Підпис накладається на сформований електронний документ (структурований файл/контейнер), що містить зафіксовані дані. У Системі зберігається підписаний документ разом з метаданими, що забезпечують можливість перевірки його цілісності та автентичності.

До Системи не вносяться відомості (дані), що становлять державну таємницю. Також у Системі не обробляються та не зберігаються документи і дані з грифом «Для службового користування» (ДСК).

5.15.9.4.2. Типові користувацькі сценарії

Таблиця. Сценарій створення (документу)

НАЗВА	Створення (документу)
ЦІЛЬ	Я, як авторизований користувач з певною користувацькою роллю, хочу створити в Системі документ певного виду, для того щоб в подальшому виконати певні спеціалізовані дії з цим документом (зберегти, редагувати та інше) та в подальшому використовувати цей документ в потрібних бізнес процесах.
АКТОРИ	Користувач з роллю якій надано право створювати документ певного виду. Система.
ПЕРЕДУМОВИ	Користувач має бути авторизованим та автентифікованим. Користувач має роль якій надано право створювати документ певного виду. Сесія користувача має бути активною.
ПІСЛЯУМОВИ	Документ певного виду створено. Створений документ доступний для виконання певних

	спеціалізованих дії з цим документом.
--	---------------------------------------

Таблиця. Сценарій перегляду (документу)

НАЗВА	Перегляд (документу)
ЦІЛЬ	Я, як авторизований користувач з певною користувацькою роллю, хочу переглянути в Системі документ певного виду, для того щоб ознайомитися з інформацією в документі.
АКТОРИ	Користувач з роллю, в якій надано право переглядати документ певного виду. Система.
ПЕРЕДУМОВИ	Користувач має бути авторизованим та автентифікованим. Користувач має роль якій надано право переглядати документ певного виду. Сесія користувача має бути активною. Документ певного виду створений та збережений в системі.
ПІСЛЯУМОВИ	Документ певного виду відкрито та переглянуто. Система повертається в стан, який передував відкриттю документа на перегляд.

Таблиця. Сценарій редагування документу

НАЗВА	Редагування документу
ЦІЛЬ	Я, як авторизований користувач з певною користувацькою роллю, хочу відредагувати документ певного виду, для того щоб в подальшому виконати певні спеціалізовані дії з цим документом та в подальшому використовувати цей документ в потрібних бізнес процесах.
АКТОРИ	Користувач з роллю, в який надано право редагувати документ певного виду. Система.

ПЕРЕДУМОВИ	<p>Користувач має бути авторизованим та автентифікованим.</p> <p>Користувач має роль якій надано право редагувати документ певного виду.</p> <p>Сесія користувача має бути активною.</p> <p>Документ певного виду створений та збережений в системі.</p>
ПІСЛЯУМОВИ	<p>Документ певного виду відредаговано.</p> <p>Система повертається в стан, який передував редагуванню документу.</p>

Таблиця. Сценарій видалення (чернетки документу)

В даному сценарії мова йде про м'яке видалення даних – процес, при якому дані не видаляються остаточно з системи, а лише позначаються як архівні, що дозволяє зберегти їх в базі даних для можливого подальшого відновлення.

НАЗВА	Видалення (чернетки документу)
ЦІЛЬ	Я, як авторизований користувач з певною користувацькою роллю, хочу видалити з відображення в Системі чернетку документу певного виду який не повинен використовуватися в загальних бізнес процесах.
АКТОРИ	Користувач з роллю, в який надано право видаляти чернетку документу певного виду. Система.
ПЕРЕДУМОВИ	<p>Користувач має бути авторизованим та автентифікованим.</p> <p>Користувач має мати право видаляти чернетку документу певного виду.</p> <p>Сесія користувача має бути активною.</p> <p>Чернетка документу певного виду створена та збережена в системі.</p>

ПІСЛЯУМОВИ	Чернетка документу певного виду помічена як видалена (але фізично не видалена з БД) та відображається в відповідному певному реєстрі або в загальному реєстрі документів в режимі “відобразити видаленні”
------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Таблиця. Сценарій відновлення чернетки
(документу)

НАЗВА	Відновлення видаленої чернетки документу
ЦІЛЬ	Я, як авторизований користувач з певною користувацькою роллю, хочу відновити в системі чернетку документу певного виду, для того щоб продовжити з ним роботу.
АКТОРИ	Користувач з роллю, в який надано право відновлювати чернетки документу певного виду. Система.
ПЕРЕДУМОВИ	Користувач має бути авторизованим та автентифікованим. Користувач має мати право відновлювати чернетки документ певного виду. Сесія користувача має бути активною. Чернетка документу певного виду видалена.
ПІСЛЯУМОВИ	З чернетки документу певного виду знята відмітка про видалення та він відображається в відповідному певному реєстрі або в загальному реєстрі документів в режимі відображення документів (крім тих, що мають статус видалених)

Таблиця. Сценарій підписання документу

НАЗВА	Підписання документу
ЦІЛЬ	Я, як авторизований користувач з відповідною роллю, хочу накласти електронний підпис на документ певного виду в Системі, щоб підтвердити його

	автентичність, цілісність та юридичну силу.
АКТОРИ	Користувач з роллю, в якій надано право підписувати документ певного виду. Система.
ПЕРЕДУМОВИ	Користувач має бути авторизованим та автентифікованим. Користувач має роль якій надано право підписувати документ певного виду. Сесія користувача має бути активною. Документ певного виду створений та збережений в системі. Користувач має дійсний електронний підпис.
ПІСЛЯУМОВИ	Документ підписано електронним підписом користувача. Система підтверджує успішне підписання та забезпечує можливість подальшого перегляду документа.

Таблиця. Сценарій створення редакції документу

НАЗВА	Редакція документу
ЦІЛЬ	Я, як авторизований користувач з відповідною роллю, хочу створити редакцію документ певного виду в Системі, щоб внести зміни у документ що знаходиться в статусі Зареєстровано.
АКТОРИ	Користувач з роллю, в якій надано право створення документ певного виду. Система.
ПЕРЕДУМОВИ	Користувач має бути авторизованим та автентифікованим. Користувач має роль якій надано право підписувати документ певного виду. Сесія користувача має бути активною. Документ певного виду створений та зареєстрований

	в системі.
ПІСЛЯУМОВИ	Створено редакцію картки документу у стані Чорнетка. У картку документу скопійовано всі дані з попередньої редакції документу доступні для редагування та видалення Система підтверджує успішне створення редакції та забезпечує можливість подальшого перегляду та редагування документа.

5.15.9.5. МОДУЛЬ “ДОВІДНИКИ ТА КЛАСИФІКАТОРИ

5.15.9.5.1. Опис та призначення

В системі мають використовуватись класифікатори, довідники, словники та бази даних, які ведуться Мінрозвитку, дані містобудівного кадастру, а також державні та галузеві класифікатори, довідники, словники та бази даних, які ведуться іншими державними органами, місцевими держадміністраціями (військовими адміністраціями), органами місцевого самоврядування.

Система має забезпечити можливість для Технічного адміністратора щодо внесення змін до класифікаторів, довідників, словників та баз даних системи.

Таблиця. Сценарій управління довідниками

НАЗВА	Управління довідниками
ЦІЛЬ	Я, як користувач з правом управління довідниками хочу здійснити з ними певні спеціалізовані дії (знайти, переглянути, додати, редагувати, видалити, блокувати, відновити, змінити та інше)
АКТОРИ	Користувач з правом управління довідниками
ПЕРЕДУМОВИ	Користувач авторизований в системі та має відповідну роль
ПІСЛЯУМОВИ	Користувач проводить дії з довідниками (знайти, переглянути, додати, редагувати, видалити,

	блокувати, відновити та інше)
--	-------------------------------

Для забезпечення цілісності та історичності даних повинні бути реалізовані наступні механізми:

- документи системи зберігають значення довідників у незмінному вигляді, незалежно від подальших змін у довідниках;
- зміни в довідниках мають версіюватися із фіксацією дати, автора та опису зміни;
- у системі повинні підтримуватися таблиці перекодування, що дозволяють зберігати зв'язки між застарілими та актуальними значеннями довідників.

5.15.9.6. МОДУЛЬ “АДМІНІСТРУВАННЯ”

5.15.9.6.1. Опис та призначення

Модуль “Адміністрування” передбачає реалізацію середовища для адміністратора Системи в частині управління користувачами, ролями, правами доступу, налаштуваннями системи та контролем доступу до електронного кабінету користувачів. Доступ до функціоналу модуля надається виключно користувачам із відповідними адміністративними правами. В цілому модуль має забезпечувати:

- управління обліковими записами користувачів електронних кабінетів;
- управління ролями та правами доступу відповідно до бізнес-процесів;
- налаштування параметрів безпеки та системних конфігурацій;
- аудит дій користувачів та контроль доступу до даних.

5.15.9.6.2. Функціональні вимоги

Модуль повинен забезпечувати повний цикл управління користувачами, включаючи управління обліковими записами в системі: блокування, анулювання та відновлення доступу.

Блокування доступу здійснюється шляхом встановлення статусу облікового запису «Заблоковано». Механізм передбачає два типи блокування:

- автоматичне (в разі появи в Системі відповідних підстав;
- адміністративне (ініціюється адміністратором у разі отримання підстав для цього).

Така дія не призводить до видалення ролей, а обліковий запис може бути розблокований. Для заблокованих облікових записів користувачів, яким були призначені ролі, система повинна забезпечувати можливість повернення до базового облікового запису, проте всі інтерфейси користувача блокуються, а система виводить повідомлення про блокування. Відновлення доступу після блокування виконується адміністратором системи після перевірки підстав.

Анулювання доступу є процесом, за якого обліковий запис отримує статус «Анульовано». Система автоматично відключає активні сеанси, анулює токени автентифікації та зберігає зв'язки користувача з даними для забезпечення цілісності бази.

Система повинна підтримувати керування ролями, що дозволяє обмежувати доступ лише в межах конкретного контексту.

Система повинна забезпечувати ведення журналу дій з адміністрування (щодо блокування, анулювання, відновлення доступу з фіксацією дати, часу, адміністратора та підстави.

Система повинна забезпечувати автоматичне інформування користувачів про блокування, анулювання, відновлення доступу через повідомлення в системі та/або на електронну пошту.

5.15.9.7. МОДУЛЬ “ГІС-СЕРВЕР”

5.15.9.7.1. Опис та призначення

Модуль “ГІС-сервер” в цілому повинен забезпечувати реалізацію можливості візуалізації даних про ОНМ, у вигляді картографічного зображення, та включати наступні можливості:

- картографічна візуалізація даних про ОНМ на картографічній підоснові, з можливістю перегляду деталізованих атрибутивних даних по кожному об'єкту за допомогою та карток об'єктів;

- підключення та візуалізація геопросторових даних, отриманих з СУБД та відкритих сервісів (за допомогою WMS/WTMS/WFS серверів);
- групування та фільтрування об'єктів у реєстрах і на карті за визначеними критеріями (наприклад: тип житла, стан придатності, територіальна прив'язка);
- підтримку та відображення метаданих для наборів геопросторових даних;
- галерею робочих шарів та базових карт для вибору зручного режиму перегляду;
- інструменти навігації (міні-карта, масштабна лінійка, панель управління відображенням шарів).

1.1.1.1. Функціональні вимоги

Система повинна забезпечувати функціонування веб-карти як інтерактивного контейнера для базових картографічних шарів, тематичних шарів з даними про ОНМ, а також підключених зовнішніх геосервісів (WMS/WMTS/WFS).

Веб-карта повинна мати визначені властивості: початковий екстент, систему координат, набір базових карт, налаштування шарів даних та параметри стилізації відображення об'єктів.

Веб-карта повинна забезпечувати базові інструменти навігації: масштабування, панорамування, вибір шару відображення, перегляд легенди, пошук об'єктів за атрибутами.

Система повинна забезпечувати можливість перегляду атрибутивної інформації по кожному об'єкту (через картку об'єкта або вікно з атрибутами) з використанням даних із реєстру.

Користувачі повинні мати змогу фільтрувати об'єкти на карті за визначеними критеріями (тип житла, стан придатності, територіальне розташування тощо) та групувати їх для зручного візуального відображення.

Для кожного шару даних повинні бути доступні метадані (опис джерела, дата актуалізації, відповідальний орган, якісні характеристики).

У публічній частині порталу повинні відображатися виключно ті об'єкти, що класифіковані як придатні для проживання ВПО, відповідно до бізнес-процесів системи.

Початкове відображення карти повинно забезпечувати час реакції не більше 3 секунд, а подальше завантаження великих обсягів даних має виконуватися асинхронно із застосуванням механізмів кешування, тайлінгу та оптимізації відображення.

Система повинна забезпечувати інтерактивне відображення наступних базових картографічних шарів:

- основна державна топографічна карта України масштабу 1:50 000;
- оглядова електронна карта України 1:50 000;
- космічні ортофотоплани “Planet Scope”
- карта OSM Standard.

5.15.9.8. МОДУЛЬ “ЗОВНІШНІ ІНТЕГРАЦІЇ”

5.15.9.8.1. Опис та призначення

Модуль “Зовнішні інтеграції” призначений для забезпечення можливості електронної інформаційної взаємодії з іншими електронними інформаційними ресурсами, системами. Система повинна мати можливість підключатися до зовнішніх систем, зокрема через Трембіту та стандартизовані API або інші механізми інтеграції.

Організація інтеграцій здійснюється відповідно до підписаних та погоджених протоколів інформаційної взаємодії (далі - протоколи) до укладених договорів про інформаційну взаємодію.

Список процесів та інтеграцій за необхідності може бути розширеним або за необхідності зміненим під час розробки.

5.15.9.8.2. Інтеграція з ДІЯ

Описання вимог до інтеграції з Системою, а саме обміну даними щодо надання публічної послуги, буде за потреби сформовано в окремому документі на етапі формування Технічного завдання.

5.15.9.8.3. Інтеграція з ICEI

Метою інтеграції з Інтегрованою системою електронної ідентифікації (ICEI id.gov.ua) є забезпечення автентифікації користувачів в Системі та реалізація механізму підписання документів. Електронна автентифікація здійснюється за допомогою електронних підписів (на файловому, хмарному чи інших захищених носіях), Дія.Підпис та BankID НБУ.

Створення електронного документа завершується накладенням користувачем електронного кабінету власного електронного підпису з дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг.

Електронні підписи, які можуть використовуватися для ідентифікації поділяються на:

- електронний підпис - дані, які додаються підписувачем до електронного документа або логічно з ними пов'язуються і використовуються ним як підпис;
- удосконалений електронний підпис (УЕП) - тип підпису, що дає змогу засвідчити згоду підписувача із змістом електронного документа, ідентифікувати підписувача, є підставою для виникнення юридичних фактів та є достовірними доказами в суді, окрім того використовується для забезпечення цілісності електронного документа;
- кваліфікований електронний підпис (КЕП) - підпис має ті самі характеристики, що і УЕП, але додатково забезпечує вищий рівень захисту, має високий рівень довіри як засіб електронної ідентифікації та прирівнюється до власноручного підпису.

Підписання всіх документів, які створюються в Системі, здійснюється з використанням сервісу "Підпис файлів".

Система повинна надавати можливість користувачам накладати електронний підпис на документи в Системі та переглядати відомості накладеного електронного підпису, в т.ч. Дія.Підпис. Система повинна надавати можливість користувачу засвідчувати свою особу при авторизації та підтверджувати документи, які користувач відправляє в Системі.

Сервіс електронного підпису повинен використовувати криптографічні бібліотеки для КЕПу, які мають працювати у вигляді окремого сервісу, до якого звертатиметься Система при реєстрації, аутентифікації та авторизації користувача. В межах Системи має відбуватись генерація документів та накладання на згенеровані чи отримані Системою документи електронним підписом одного чи декількох користувачів.

Система повинна давати можливість накладати електронний підпис на файли у форматі PDF, а при друкуванні підписаного файлу відображати дані про підписанта.

Сервіс повинен давати можливість накладання електронного підпису без ручного втручання. Процес авторизації та накладення електронного повинен відбуватись в тому числі на основі засобів посиленого сертифікату відкритого ключа КЕП та захищеного носія особистих ключів.

5.15.9.8.4. Інтеграція з ЄІССС

Метою інтеграції з ЄІССС (Єдина інформаційна система соціальної сфери) є отримання інформації, необхідної для:

- отримання достовірної інформації про ВПО, перевірки статусу ВПО та фактичного обліку;
- актуалізації відомостей про зміни статусів ВПО (зняття з обліку, припинення довідки тощо).

Для обміну даними використовується протокол SOAP (згідно з WSDL специфікаціями, опублікованими ЄІССС). Для забезпечення такого обміну даними формується Протокол двосторонньої взаємодії, який визначає порядок, періодичність та обсяг даних. Передбачена модальність:

1. Початкове вивантаження даних про всіх зареєстрованих ВПО.
2. Подальше періодичне оновлення інформації.

Таблиця. Інтеграційні функції

№	Функціонал	Опис
1	Отримання інформації про ВПО	Пошук та отримання даних про конкретну ВПО (персональні дані, дані довідки ВПО). Метод GetDisplacedPerson

2	Ініціювання отримання змін у інформації про ВПО	Формування запиту на отримання інформації про зміни у інформації про ВПО за визначений період, повертає ідентифікатор запиту. Метод GetDisplacedDelta
3	Отримання результатів запиту на зміни	Отримання результату обробки запиту на отримання змін у інформації про ВПО, повертає перелік файлів-відповідей. Метод GetDeltaAnswer

5.15.9.8.5. Інтеграція з ЄДР

Метою інтеграції з ЄДР (Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань) є отримання інформації, необхідної для:

- ідентифікації юридичних осіб, які беруть участь у бізнес-процесах;
- підтвердження відповідності користувачів-юридичних осіб даним державного реєстру під час онбордингу через систему електронної ідентифікації (ICEI);
- перевірки актуального статусу юридичної особи за кодом ЄДРПОУ (діюча, ліквідована, призупинена), щоб унеможливити доступ до Системи суб'єктів із невалідним статусом;
- підтвердження повноважень посадових осіб, які взаємодіють із Системою від імені органів державної влади чи органів місцевого самоврядування.

Система повинна забезпечувати автоматичне співставлення даних ICEI з відомостями з ЄДР. У разі успішного підтвердження користувач-юридична особа завершує процедуру онбордингу та отримує відповідний рольовий доступ.

Таблиця. Інтеграційні функції

№	Функціонал	Опис
---	------------	------

1	Отримання відомостей про юридичну особу	Пошук та завантаження даних про юридичну особу за кодом ЄДРПОУ (найменування, статус, адреса, керівник, дата реєстрації).
2	Перевірка статусу юридичної особи	Визначення, чи є юридична особа діючою, у стані припинення, ліквідованою або призупиненою.
3	Отримання даних про уповноважених осіб	Завантаження інформації про керівників та інших представників юридичної особи, що мають право діяти від її імені.
4	Перегляд історії змін	Отримання інформації про зміни у реєстраційних даних (керівники, адреси, статуси тощо).

5.15.9.8.6. Інтеграція з ЄДРА та ЄДРАТО

Метою інтеграції з ЄДРА (Єдиний державний реєстр адрес) та ЄДРАТО (Єдиний державний реєстр адміністративно-територіальних об'єктів) є отримання достовірної інформації про адресу ОНМ для створення відповідного запису в Системі про ОНМ.

Для обміну даними використовуються відповідні API. Передбачена наступна модальність:

- отримання інформації про адміністративно-територіальні одиниці;
- пошук вулиць, адрес та об'єктів за текстовим запитом;
- отримання історії змін адресних об'єктів.

Таблиця. Інтеграційні функції

№	Функціонал	Опис
1	Отримання даних про адміністративно-територіальні одиниці	Завантаження інформації про конкретну адміністративно-територіальну одиницю. Метод: Edrato

2	Перелік об'єктів за ідентифікатором вищого рівня	Отримання списку об'єктів за глобальним ідентифікатором об'єкта вищого рівня. Метод: EdratoList
3	Отримання списку вулиць	Завантаження вулиць за ідентифікатором адміністративної одиниці. Метод: StreetList
4	Інформація з ЄДРА про об'єкти	Отримання даних про об'єкти за їх [id]. Метод: Edra
5	Пошук об'єктів за координатами або полігоном	Отримання списку об'єктів за полігоном, координатами точки або ідентифікатором об'єкта вищого рівня. Метод: Adress
6	Повнотекстовий пошук об'єктів	Отримання інформації за текстовим запитом в межах населеного пункту з вказанням типу об'єкта. Метод: Geocoding
7	Пошук адміністративної одиниці за текстом	Отримання даних про адміністративно-територіальну одиницю за текстовим запитом із зазначенням типів об'єктів. Метод: GeocodingEdrato
8	Історія змін адрес	Вивантаження історії об'єктів у вигляді архіву за містом, вулицями та адресами за вказаний період. Метод: EdraHistory
9	Надходження нової заявки на зміну/додавання адрес	API отримує нову заявку, завантажує дані в базу і повертає номер заявки та її статус. Метод: Appeal
10	Отримання статусу заявки	Повертає інформацію по історії змін статусів заявки, а у випадку відхилення – причину відхилення. Метод: Appeal-status

5.15.9.8.7. Інтеграція з ЄДЕССБ (з РБС)

Метою інтеграції з РБС (Реєстр будівель та споруд) є отримання достовірної інформації, необхідної для:

- ідентифікації ОНМ як будівлі в РБС;

- підтвердження базових та додаткових характеристик об'єкта;
- завантаження ТЕП, що використовуються у бізнес-процесах Системи.

Таблиця. Інтеграційні функції

№	Функціонал	Опис
1	Отримання основних характеристик ОНМ	Завантаження загальної інформації об'єкта будівництва (Реєстраційний номер у Реєстрі будівельної діяльності, Найменування об'єкта нерухомого майна, Адреса об'єкта , дані щодо земельної ділянки, PDF-документ Технічний паспорт, дані щодо поточного стану ОНМ (чи перебуває він у стані проектування чи будівництва)
2	Отримання додаткових характеристик об'єкта	Відомості про технічне обстеження, енергетичний сертифікат,, інженерне обладнання, тощо
3	Підсумкові показники об'єкта нерухомого майна	Ідентифікатори об'єктів будівництва, Об'єкти технічної інвентаризації (Об'єкт, ТЕП),

Під час розробки технічного завдання, розробнику провести консультації з ДП “Адміністратор містобудівного кадастру на державному рівні” для визначення технічної та юридичної складової інтеграції

5.15.9.8.8. Інтеграція з ДРРП

Метою інтеграції з ДРРП (Державний реєстр речових прав на нерухоме майно) є отримання достовірної інформації, необхідної для:

- надання користувачу ролі Власника ОНМ;
- створення ОНМ у базі даних Системи з прив'язкою до реєстраційних номерів; отримання актуальної інформації про зареєстровані речові права та їх обтяження у режимі реального часу через Систему

електронної взаємодії державних електронних інформаційних ресурсів «Трембіта».

Для обміну даними використовується сервіс ДРРП, який, залежно від пошукових параметрів, забезпечує вивантаження даних про перелік нерухомого майна або інформацію про зареєстровані речові права та їх обтяження.

Таблиця. Інтеграційні функції

№	Функціонал	Опис
1	Надання ролі Власник а ОНМ	Пошук ОНМ за обліковими даними користувача (РНОКПП, серія та номер документу, УНЗР). Передача частки користувача з валідацією на рівні Системи (зокрема підрахунок загальної частки у випадках, коли записів одному користувачу по одному ОНМ більше ніж один).
2	Створення об'єкта ОНМ у Системі	Пошук ОНМ за адресою, завантаження та передача в Систему реєстраційного номеру ОНМ.
3	Формування співвласників ОНМ	Пошук співвласників по об'єкту, передача частки користувачів та підрахунок загальної частки кожного співвласника (у випадках, коли записів одному співвласнику по одному ОНМ більше ніж один).
4	Отримання даних про речові права та обтяження	Передача актуальної інформації у режимі реального часу за запитом від Системи через «Трембіту». Сервіс повертає відомості про перелік нерухомого майна або дані про зареєстровані права та обтяження.

5.15.9.8.9. Інтеграція з ІКІС ПФУ

Метою інтеграції з ІКІС ПФУ (Інтегрована комплексна інформаційна система Пенсійного фонду України) в складі ЄІССС є створення API, яке забезпечуватиме надання необхідних відомостей для обліку та контролю забезпечення ВПО житлом:

- інформування органів ПФУ інформації з протоколів засідань координаційних комісій щодо ОНМ, які використовуються для проживання ВПО;
- отримання актуальної інформації про прийняті рішення координаційних комісій щодо надання ВПО житла.

5.15.9.8.10. Інтеграція з ДЗК

Метою інтеграції з ДЗК (Державний земельний кадастр) є отримання достовірної інформації про земельні ділянки, необхідної для:

- отримання характеристик земельних ділянок для будівництва об'єктів нерухомого майна для проживання ВПО та/або розміщення тимчасових споруд, їх комплексів, призначених для життєзабезпечення (тимчасового проживання та обслуговування) ВПО);
- підтвердження правового статусу, цільового призначення, площі та власності таких земельних ділянок.

Таблиця. Інтеграційні функції

№	Функціонал	Опис
1	Отримання інформації за кадастровим номером	Повернення даних про конкретну земельну ділянку: категорія земель, цільове призначення, код і опис, фактичне використання, площа, одиниця виміру, власність, координати (ppoint, zoom_to).
2	Візуалізація геометрії земельних ділянок	Отримання геометрії (координати, полігон) та відображення її на карті. Геометрія повертається лише для тих ділянок, що пов'язані з об'єктами ОНМ і внесені до Системи ВПО.

5.15.9.8.11. Інтеграція з Єдиним державним веб-порталом відкритих даних

Метою інтеграції з Єдиним державним веб-порталом відкритих даних (data.gov.ua) є забезпечення виконання вимог постанови КМУ №835 від

21.10.2015 щодо обов'язкового оприлюднення наборів публічної інформації у формі відкритих даних.

Система повинна забезпечувати автоматизовану публікацію та оновлення відкритих даних через API порталу або шляхом завантаження наборів у машиночитаних форматах (CSV, JSON, XML).

Передача здійснюється відповідно до визначеного переліку наборів, з урахуванням вимог до структури, метаданих (паспортів наборів даних) та періодичності оновлення.

Таблиця. Інтеграційні функції

№	Функціонал	Опис
1	Формування наборів даних	Автоматизоване формування даних щодо забезпечення ВПО житлом (кількість об'єктів, придатних для проживання).
2	Передача даних на портал	Публікація та регулярне оновлення зазначених статистичних даних через API порталу data.gov.ua.

Перелік наборів даних, що передаються на портал data.gov.ua, може бути уточнений та розширений на етапі розробки технічного завдання.

5.15.9.9. МОДУЛЬ “CMS”

5.15.9.9.1. Опис та призначення

Модуль “CMS” (система управління контентом) має забезпечувати можливість створення, редагування, публікацію, модерацію та управління інформаційними ресурсами, що відображаються в електронних кабінетах користувачів та на публічному порталі. Система має забезпечувати контроль версій, архівування, індексацію та централізоване управління контентом. Система також має забезпечувати централізоване управління контентом та в тому числі:

- внесення, редагування та публікацію контенту лише користувачами із відповідними ролями;
- контроль версій та збереження історії змін контенту;

- керування метаданими контенту, що використовуються для пошуку та фільтрації;
- пошук контенту за ключовими словами, метаданими, категоріями та датою створення;
- архівування та резервне копіювання контенту відповідно до політики збереження даних.

5.15.9.10. МОДУЛЬ “ВА”

5.15.9.10.1. Опис та призначення

Модуль “ВА” (бізнес-аналітики) має забезпечувати функціональність збору, обробки та аналітичної обробки даних, що накопичуються в Системі, для підтримки прийняття управлінських рішень, моніторингу та звітності щодо забезпечення ВПО житлом. Основними функціями є:

- агрегація даних в межах Системи;
- формування аналітичних звітів у вигляді таблиць, діаграм, графіків для різних рівнів користувачів;
- можливість побудови кастомізованих звітів за обраними параметрами (територія, період, тип житла, тощо);
- підтримка експорту аналітичних даних у формат PDF, XLSX, CSV, JSON;
- інтерактивна візуалізація просторових даних на карті з накладенням аналітичних шарів (розподіл заяві від ВПО, стан об’єктів житла, тощо)
- налаштування системи оповіщень та інформування відповідальних осіб про критичні зміни у показниках.

5.15.9.11. МОДУЛЬ “ДОКУМЕНТАЦІЯ”

5.15.9.11.1. Опис та призначення

Модуль “Документація” призначений для централізованого зберігання, управління та надання користувачам Системи актуальних інструкцій, довідкових матеріалів та методичних документів, що забезпечують ефективну роботу з Системою. Основні функції:

- зберігання текстових інструкцій і документів із підтримкою гнучкого форматування (заголовки, списки, посилання, цитати, виділення тощо). Для представлення контенту система має

підтримувати Markdown як універсальний формат зберігання, але користувачам повинен бути доступний WYSIWYG-редактор, що дозволяє працювати з текстом у режимі «що бачиш, те й отримаєш» без необхідності знати синтаксис розмітки. WYSIWYG-модуль має забезпечувати автоматичне перетворення введеного тексту у валідний Markdown/HTML та коректне відображення його у системі.;

- функціонал створення, редагування, видалення та публікації інструкцій уповноваженими користувачами з роллю Адміністратора;
- підтримка версійності, де кожна зміна документа фіксується як окрема версія із зазначенням дати, автора та опису змін, що дозволяє відстежувати історію редагувань та при необхідності відновлювати попередні версії;
- можливість класифікації та категоризації документів для полегшення навігації та пошуку;
- пошук за ключовими словами, категоріями та змістом документів із використанням повнотекстового та семантичного пошуку. Для цього система має підтримувати інтеграцію з пошуковими рушіями (наприклад, Elasticsearch) з відповідними мовними аналізаторами, стемінгом, синонімічними словниками та можливістю розширеного пошуку за атрибутами документів..
- відображення документації у вигляді відформатованого HTML з урахуванням Markdown-розмітки для зручності читання.
- керування правами доступу до окремих документів або категорій на основі ролей користувачів системи.
- експорт інструкцій та документів у формат PDF із збереженням форматування для офлайн перегляду, друку та поширення.

6. ВИМОГИ ДО СУПРОВОДУ ТА ОБСЛУГОВУВАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

6.1. Вимоги до гарантійної підтримки

Гарантійний термін має становити не менше шести місяців, починаючи від дати підписання акта приймання-передачі робіт за останнім етапом

надання послуг відповідно до календарного плану, та розгортання програмного забезпечення на ресурсах набувача.

Послуги з гарантійного обслуговування містять:

- усунення недоліків Системи Розробником ПЗ (послуги з усунення несправностей);
- консультування відповідальних осіб з питань стосовно експлуатації, використання, встановлення та налаштування програмного забезпечення. Консультації можуть надаватись телефоном та/або електронною поштою;
- відновлення працездатності Системи під час використання, наприклад, у разі відмови роботи Системи загалом або її компонентів внаслідок оновлень або змін, які були здійснені Розробником ПЗ;
- відновлення пошкоджених даних за умови, що вони були пошкоджені внаслідок несправності програмного забезпечення, наданого Розробником ПЗ;
- надання нових версій функціоналу Системи (передбачає оновлення функцій Системи, оновлення даних Системи та оновлення інструкцій користувачів Системи);
- коригування експлуатаційної документації відповідно до змін, що були внесені до програмного забезпечення через усунення вказаних недоліків.

Із метою забезпечення надання послуг Розробником ПЗ має бути сформований перелік контактних (відповідальних) осіб, наданий доступ до стандартизованих сервісів клієнтської підтримки чи виділені канали.

Пропозиції щодо вартості гарантійної підтримки та умов її надання зазначає Розробником ПЗ у комерційній пропозиції. Послуги з гарантійної підтримки можуть бути:

- термінові;
- регламентні;
- відповідно до заявок (інцидентів).

Реагування на інциденти Системи має відбуватися як за зверненням Технічного адміністратора, так і без нього у випадку виявлення інциденту Розробником ПЗ та неможливістю погодження взаємодії з боку Сторін (відсутність зв'язку, неробочий час тощо).

6.2. Вимоги до навчання користувачів

Навчання користувачів має забезпечувати підготовку адміністраторів, операторів і кінцевих користувачів з урахуванням їхніх ролей. Воно може проводитися очно або дистанційно та має супроводжуватися навчальними матеріалами у вигляді інструкцій та відеоінструкцій, а також доступом до онлайн-бази знань.

Програма навчання має охоплювати базові та розширені сценарії роботи з системою, включно з налаштуваннями, управлінням доступом та використанням інтерфейсу. Після навчання користувачі повинні мати можливість отримати консультації через службу технічної підтримки, а при впровадженні оновлень має проводитися додаткове навчання.

В таку програму також включається розробка User Guide з покроковими інструкціями та відеоуроків (Video Tutorials) для користувачів-початківців, щоб забезпечити швидкий і зручний старт роботи з системою.

6.3. Вимоги до документації

Оформлення документації здійснюється Розробником ПЗ. Документація повинна бути повною, інформативною, зрозумілою, структурованою, зручною для читання, достатньою, однозначною та несуперечливою (повинні використовуватися тотожні терміни, визначення, ідентифікатори тощо).

Всі примірники документації передаються Замовнику у паперовому (3 примірника) та електронному (.doc та .pdf форматах) виглядах. Документація має вестись українською мовою, надаватись на електронних носіях (оптичному диску або флеш – носію) та відповідати вимогам відповідних стандартів ЕСПД та ДСТУ. У всіх документах повинні відслідковуватися варіантів, версій та редакцій.

Розроблене ПЗ повинно мати наступну проектну та експлуатаційну документацію:

- Технічне завдання;
- Програма та методика випробувань;
- Протокол випробувань та інших тестувань;
- Інструкція Адміністратора;
- Інструкція Технічного адміністратора;

- Інструкції Користувачів (відповідно до кожної ролі);
- Інструкція з резервного копіювання та відтворення даних;
- Інструкція з розгортання систем;
- Інструкція з архівування та відновлення.

Програмний код повинен супроводжуватись детальною проектною документацією, що описує основні компоненти, архітектуру системи, та її ключові функції.

Програмний код повинен містити коментарі, що пояснюють його основні блоки, логіку виконання і призначення кожної значущої частини. Коментарі повинні бути написані зрозумілою мовою і мати чіткий зв'язок з відповідними частинами коду.

Кожна функція або метод повинні мати коментар, що містить:

- опис призначення функції;
- пояснення параметрів, які вона приймає, та їх типи;
- опис повернутого значення, якщо таке є;
- опис можливих виключень або помилок, що можуть виникнути під час виконання.

Оновлення програмної документації передбачає:

- всі зміни в коді повинні супроводжуватися відповідними оновленнями в документації та коментарях;
- застарілі коментарі або не актуальна документація повинні бути видалені або виправлені у разі зміни логіки коду.

Ревізія та перевірка коду передбачає:

- проведення ревізії коду перед завершенням розробки, для перевірки відповідності документації фактичному стану коду;
- перевірка якості коментарів та їх відповідність функціоналу, який вони пояснюють.

Документація має бути виконана з урахуванням вимог Постанови КМУ від 21.02.2025 №205 “Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації”.

7. ВИМОГИ ДО ПРИЙМАННЯ ЗАСОБУ ІНФОРМАТИЗАЦІЇ

7.1. Вимоги до проведення випробувань

Перед запуском системи в експлуатацію повинно бути проведено навантажувальне тестування, що підтвердить відповідність вимогам до продуктивності та масштабованості. Результати тестування повинні бути задокументовані.

Тестування повинно включати сценарії з різними рівнями навантаження, включаючи середнє, пікове та стресове навантаження, для виявлення можливих проблемних місць у системі.

Критичний функціонал Системи має бути покритий автоматизованими тестами (unit, integration, API, UI), що забезпечує відтворюваність результатів та контроль стабільності роботи при змінах у програмному коді.

Рівень покриття автотестами та їх результати повинні бути задокументовані та надані приймальній комісії як частина випробувальної документації.

7.2. Вимоги до передачі результатів виконаних робіт

Програмне забезпечення системи є об'єктом права державної власності. Виключні майнові права на програмне забезпечення належать державі в особі Мінрозвитку.

Проведення приймальних випробувань засобу інформатизації або його компонентів передбачає утворення Замовником комісії, з залученням представників організації Розробника ПЗ, для проведення приймальних випробувань Системи.

Обробка персональних даних в електронній Системі повинна здійснюватись з дотриманням вимог Законів України “Про захист персональних даних” і “Про електронні довірчі послуги”.

Після запуску в експлуатацію Система повинна бути обладнана інструментами моніторингу продуктивності, що дозволяють відстежувати ключові показники продуктивності в реальному часі та виявляти потенційні проблеми на ранніх етапах.

Інструменти моніторингу повинні забезпечувати збір та аналіз даних, таких як середній час відгуку, пропускна здатність, використання ресурсів і кількість активних користувачів.